

**硕** **士** **学** **位** **论** **文**

**题** **目:** 基于混沌的图像加密以及优化方案研究

**研** **究** **生** 肖 涛 **专** **业** 电子信息 **指导教师** 李齐良 教授

**完成日期** 2024.05.25

中国知网 https:Www.cnki . net

杭州电子科技大学硕士学位论文

基于混沌的图像加密以及优化方案研究

研 究 生： 肖 涛

指导教师： 李齐良 教授

2024 年 5 月

中国知网 https:Www.cnki . net

**Dissertation Submitted to Hangzhou Dianzi University for the Degree of Master**

**Chaos based image encryption and optimization schemes**

**Candidate: Xiao Tao**

**Supervisor: Prof. Li Qiliang**

**May, 2024**

中国知网 https:Www.cnki . net

摘要

近年来，互联网技术日新月异，图像已经变成关键的信息传播载体。但由 于其在网络上的广泛分布和存储以及互联网环境的开放性和不稳定性，图像信 息易受窃取或篡改，特别是在敏感领域，信息泄露会导致严重后果。因此， 在 通过互联网等不安全途径传输时，确保图像内容的安全显得极其重要。

图像作为二维或三维数据，其相邻像素之间具有较强的相关性，且图像数 据量大、数据冗余程度高。混沌的伪随机性、初值和参数的敏感性，使它具备 优化图像加密算法的能力。所以，基于混沌的图像加解密算法近年来得到了广 泛青睐，并且在实际的应用中不可或缺。本文针对混沌图像加密算法设计、混 沌系统设计、光混沌系统的实现以及加密图像优化几个方面，并分析了国内外 的文献后，提出了基于混沌和激光混沌的图像加密系统。具体内容如下。

一种基于 Lorenz 超混沌和循环 DNA 编解码的图象加密方案。在该方案中， 加密过程分两步：置乱和扩散。在图像置乱阶段，图像被转化为比特信息流，

然后通过所提出的 LTM 混沌与 Fisher-Yates 洗牌算法相结合，对比特流从头排 序并重构图像。在扩散阶段，论文将 Lorenz 超混沌融入 DNA 编码过程中。利 用 Lorenz 超混沌生成的随机序列与图像像素值进行 DNA 运算，或者依据这些 随机序列决定像素值的 DNA 编码规则，对经过置乱的图像进行循环 DNA 加密。 经过这两步骤， 图像能够被很好的加密隐藏。并且通过多轮仿真和安全性测试， 论文证明了此加密系统具有较高的保密性和优秀的加密性能。

一种结合光混沌置乱、DNA 扩散和多目标粒子群优化算法的图像加密方案。 该方案利用一个主激光器（ML）发射激光至两组附属激光器（TPSL）发出两 个相同的的混沌信号，用作加密图像的伪随机序列。接着，论文使用伪随机序 列对图像序列排序和 zigzag 算法扰乱，然后将图像分块后，依次进行 DNA 加 密。将所有得到的加密图像视为整个群体，其中的每个粒子对应一个加密后的 图像。设置适应度函数后，通过多目标粒子群算法（简称 MOPSO）循环优化， 然后获取最佳的粒子群位置。在 MOPSO 算法中论文设计了帕累托优势存储库 和适当的遗传因子以获得最大的搜索范围和最佳的收敛效果。经过上述步骤后 即可得到最佳的加密图像。通过对该方案算法的一系列安全性测试， 结果表明 该方案所提出的加密算法具有良好的保密性。

关键词：混沌系统、图像加密、激光混沌、图像 DNA 编码、多目标粒子群优 化

I

中国知网 https:Www.cnki . net

**ABSTRACT**

With the rapid advancement of internet and networking technologies, images have become a pivotal medium for information exchange. However, due to their extensive circulation and storage on the web, coupled with the openness and inherent insecurity of the internet environment, image information is highly susceptible to theft or tampering, particularly in sensitive domains such as politics, economics, and national security, where leaks can result in significant damage. Consequently, ensuring the security of image content during transmission over insecure channels like the internet is an extremely crucial task.

Images, as two-dimensional or three-dimensional data, exhibit strong correlations among neighboring pixels and typically have large data volumes with high degrees of redundancy. The pseudo-randomness, sensitivity to initial conditions and parameters, and complex dynamic behavior inherent in chaotic systems make them well-suited for optimizing image encryption algorithms. Consequently, chaos-based image encryption algorithms have been extensively researched in recent years and play a significant role in practical applications. This paper focuses on the design of chaos- based image encryption algorithms, the design of chaotic systems, the implementation of optical chaos systems, and optimization of encrypted images. Building upon domestic and international research, it proposes a novel image encryption system that integrates chaos and optical chaos. The specific research contents are outlined as follows.

A cryptographic scheme for image encryption based on hyper-chaos from the Lorenz system and cyclic DNA coding involves two primary stages: permutation and diffusion. In the permutation phase, the image is converted into a bitstream, which is then rearranged and restructured by combining a proposed implementation of LTM chaos with the Fisher-Yates shuffling algorithm, thereby scrambling the bitstream data representation of the image. In the diffusion stage, the process integrates hyper-chaos from the Lorenz system into the DNA encoding procedure. Random sequences generated by the Lorenz hyper-chaotic system are utilized to perform DNA operations on the pixel values or to dictate the rules for DNA coding of the pixel values. The permuted image undergoes cyclic DNA encryption according to these randomly derived patterns. After these two steps, the image is effectively concealed and encrypted. Extensive rounds of simulations and security tests have been conducted to

II

中国知网 https:Www.cnki . net

demonstrate that this encryption system possesses a high level of confidentiality and exhibits superior encryption performance.

A novel image encryption scheme combines optical chaos permutation, DNA diffusion, and a Multi-objective Particle Swarm Optimization (MOPSO) algorithm. The method employs a master laser (ML) to drive two pairs of slave lasers (TPSL), which generate dual synchronous chaotic signals serving as pseudo-random sequences for encrypting the image. These pseudo-random sequences are then utilized to reorder the image sequence and apply zigzag scrambling. Subsequently, the scrambled image is partitioned into blocks, each of which undergoes DNA encryption in turn. All resulting encrypted images are treated as a single population in the MOPSO framework, with each particle representing an encrypted image block. With a fitness function defined, the MOPSO algorithm iteratively identifies the optimal positions within the particle swarm through multiple cycles, employing a Pareto archive and judiciously chosen genetic factors to maximize search space coverage and achieve optimal convergence properties. Upon completion of these steps, the best-encrypted images are obtained. A series of security tests conducted on this proposed scheme have shown that its encryption algorithm possesses robust confidentiality.

**Keywords** ：Chaos Systems, image Encryption, laser Chaos, image DNA Encoding, Multi-objective Particle Swarm Optimization

III

中国知网 https:Www.cnki . net

目 录

[第一章 引言 1](#bookmark1)

[1.1 研究背景与意义 1](#bookmark2)

[1.2 光混沌研究现状 2](#bookmark3)

[1.3 图像加密研究现状 3](#bookmark4)

[1.4 论文的主要工作与结构 4](#bookmark5)

[1.4.1 论文主要研究内容 5](#bookmark6)

[1.4.2 论文的结构安排 6](#bookmark7)

[第二章 混沌与图像加密理论基础 8](#bookmark8)

[2.1 混沌理论 8](#bookmark9)

[2.1.1 混沌系统的定义 8](#bookmark10)

[2.1.2 混沌的性质 9](#bookmark11)

[2.2 基于半导体激光器的混沌信号生成 10](#bookmark12)

[2.3 混沌图像加密 13](#bookmark13)

[2.3.1 混沌图像加密流程 13](#bookmark14)

[2.3.2 Fisher-Yates 洗牌算法 14](#bookmark15)

[2.3.3 Lorenz 超混沌系统 14](#bookmark16)

[2.3.4 DNA 编码和计算 15](#bookmark17)

[2.3.5 多目标粒子群优化算法 16](#bookmark18)

[2.4 本章小结 18](#bookmark19)

[第三章 基于 Lorenz 超混沌和循环 DNA 编码的图像加密方案 20](#bookmark20)

[3.1 加密系统模型 20](#bookmark21)

[3.2 混沌系统分析 20](#bookmark22)

[3.3 图像加密流程 22](#bookmark23)

[3.3.1 密钥以及混沌初始值生成 22](#bookmark24)

[3.3.2 Fisher-Yates 算法置乱 23](#bookmark25)

[3.3.3 DNA 编码扩散机制 24](#bookmark26)

[3.4 图像解密过程 25](#bookmark27)

[3.5 算法安全性分析 26](#bookmark28)

[3.5.1 密钥空间与敏感性分析 27](#bookmark29)

[3.5.2 直方图分析 28](#bookmark30)

[3.5.3 图像像素相关性分析 29](#bookmark31)

[3.5.4 图像熵分析 30](#bookmark32)

[3.5.5 抗差分攻击测试 31](#bookmark33)

[3.5.6 抗噪声测试 32](#bookmark34)

中国知网 https:Www.cnki . net

[3.5.7 抗裁剪测试 33](#bookmark35)

[3.6 本章小结 35](#bookmark36)

[第四章 结合光混沌置乱、DNA 扩散和多目标粒子群优化算法的图像](#bookmark37)

[加密方案 36](#bookmark37)

[4.1 加密系统模型 36](#bookmark38)

[4.2 激光器动力学特性 38](#bookmark39)

[4.3 图像加密算法 43](#bookmark40)

[4.3.1 密钥生成 43](#bookmark41)

[4.3.2 混沌置乱 44](#bookmark42)

[4.3.3 DNA 加密 45](#bookmark43)

[4.3.4 多目标粒子群算法应用 46](#bookmark44)

[4.3.5 解密流程 48](#bookmark45)

[4.4 加密算法安全性分析 49](#bookmark46)

[4.4.1 密钥空间以及密钥敏感性测试 50](#bookmark47)

[4.4.2 直方图测试 51](#bookmark48)

[4.4.3 像素相关性测试 52](#bookmark49)

[4.4.4 图像熵分析 53](#bookmark50)

[4.4.5 抗差分攻击分析 54](#bookmark51)

[4.4.6 X2 测试结果 55](#bookmark52)

[4.4.7 抗噪声和裁剪攻击 55](#bookmark53)

[4.5 本章小结 57](#bookmark54)

[第五章 总结与展望 59](#bookmark55)

[5.1 总结 59](#bookmark56)

[5.2 展望 61](#bookmark57)

[参考文献 62](#bookmark58)

中国知网 https:Www.cnki . net

第一章 引言

1.1 研究背景与意义

近年来，随着互联网和网络技术的飞速发展，人们能够在互联网上通过语 音、视频、图像等媒介进行信息交换。其中， 图像作为一种重要的信息载体， 在网络传播和存储中变得日益流行。然而，由于互联网的实时便捷和信息开放 的特性，使得互联网上的信息往往杂乱且容易被窃取。尤其是在政治、经济、 国家安全等信息敏感的领域，信息泄露或遭到篡改无疑会造成巨大的损失。由 于图像经常需要通过互联网等不安全的渠道进行传输，因此保护图像内容成为 一项至关重要的任务。 在图像安全技术中，图像加密是保护图像的重要措施， 在学术和生活中有很好的研究价值和应用价值。

图像加密是一种可以把轻易识别的图像变换成无法辨认的样式的方法。从 提出至今，加密算法已经发展得相当成熟。 密码学中的加密技术有两类：密钥 对称的加密方法与密钥不对称的加密方法。早期的数据加密标准（DES）、高级 加密标准（AES）以及 RSA 算法具有较高的密码安全性，但这些主要适用于数 据冗余度较低的一维文本数据。然而，在处理图像数据时，由于图像本质上是 二维或三维的数据结构，其中相邻像素间存在着显著的相关性，并且图像数据 量庞大、冗余度较高， 当我们运用上述传统的数据加密算法时，往往会遭遇一 系列问题。例如加密的效率不高，延时高等。从而无法实现图像传输的实时性 和安全性[1]。随后，混沌与图像加密算法结合的方法开始出现。由于混沌的伪 随机性、初值以及参数的敏感性和复杂的动力学行为，使它具备优化传统图像 加密算法的能力。使用混沌进行图像加密可以克服密钥空间不足，信息熵低等 问题。因此，基于混沌的图像加密算法在图像通信领域起着重要的作用。

在早期的图像加密技术中，主要采用的是电混沌方法， 这类方法在电路上 易于实现，并可通过数学模型进行仿真实现。 在混沌理论中，几种广泛研究并 应用的混沌映射有 Logistic 映射、Tent 映射以及 Sine 映射，它们均属于一维混 沌系统的典型代表，即这些映射所处理的是单个变量在连续迭代过程中的复杂 动力学行为[2-4]。然而，这类方法存在一些缺点，如电路的高成本、高衰减以及 较低的复杂度。

随着激光器非线性动力学的不断研究，半导体激光器产生的光混沌信号受 到众多学者的青睐。实验结果显示，半导体激光器输出的光混沌信号具有几大

1

中国知网 https:Www.cnki . net

长处，例如带宽和复杂度较高，损耗较低等[5] ，这不仅解决了传统电混沌存在 的问题，而且非常适合于图像加密的相关研究和应用[6]。

因此，基于激光混沌的图像加密方案展现出极高的应用潜力，尤其是在对 信息高效传输有比较大的需求的当下，利用光混沌所实现的图像加密算法有望 成为热门研究对象。然而， 当前对光混沌实现的图像加密算法相对来说并不多， 而且大多还处于理论研究阶段。利用激光混沌实现图像的加密，未来可期。

1.2 光混沌研究现状

激光器为非线性系统，虽然能够产生稳态信号，但它内部普遍存在不稳定 性。在激光器的应用中，光反馈难以避免。激光的混沌现象是激光器的一种比 较特别的形态，其动态特征可以通过速率方程表示，但在时域上，其表现为类 似于噪声的随机信号。

最初阶段，激光器动力学理论和混沌理论各自发展， 一直到 1975 年，

Haken 团队在研究推导半导体激光器的非线性方程时发现激光器和混沌之间存 在联系[7] 。Ikeda 等人在 1979 年提出了时延反馈的混沌模型[8] 。最初的重点更多 的是放在怎么去阻止光反馈的产生以及防止外部光注入上面，从而保证激光器 平稳运行[9]。然而，1980 年，R. Lang 和 K. Kobayashi 观察到了光反馈如何导致 激光器的不稳定性并产生混沌现象。他们进行了全面的理论推导，从而建立了 描述激光混沌的 L-K 方程[10]。通常来说，为了使半导体激光器产生混沌光输出， 需要借用外部的扰动机制，这些扰动可以体现在诸如外部光注入、光反馈及光 电反馈等多种方式上，以激活激光器内部的非线性动态行为。

时延反馈光通信系统中时延特征泄露会导致系统安全问题[11] 。Rontani D 等 人研究得出反馈的速率中等并且注入电流让激光弛豫振荡周期接近延迟时，时 延识别变得极其困难，所以就能提升使用外腔激光器的混沌通信的安全性[12] 。 SongSui Li 等人研究受光纤布拉格光栅 (FBG) 分布式反馈影响的半导体激光器 的混沌动力学。因为沿着 FBG 的分布反射，相比于传统的镜面反馈技术，FBG （光纤布拉格光栅）反馈方法在混沌信号产生的反馈延迟时间控制方面展现了 更为优越的性能[13] 。提升混沌输出的健壮性也同样很重要。Rontani D 等人通过 实验在数值上证明了半导体激光器在相位共轭反馈( PCF )下可以表现出混沌复 杂性的增强，对于安全通信和随机数生成的应用至关重要[14] 。Nianqiang Li 等 人已经证实，通过将具备显著线宽增强特性的外腔激光器对第二个未进行注入 锁定的半导体激光器进行光学注入，能够在消除时延效应的同时，有效提升混 沌动力学的复杂性[15] 。Bogris 等人提出，在由半导体激光器构建的、具有延迟

2

中国知网 https:Www.cnki . net

光反馈机制的混沌系统框架下，可以利用反馈相位作为安全混沌通信的关键密 钥来源，并证明了窃听者即使配备了相同的混沌设备，也无法同步， 且无法在 不知道相位变化时提取信息[16] 。Hu Hanping 等研究者设计了一种基于可变参数 电光振荡器的混沌系统构架，该系统能够在较低增益水平下顺利进入混沌状态， 并且具备有效掩盖延迟时间的能力[17] 。Meitong Yu 提出了一种差分反馈电光相 位混沌系统来产生超宽带光学混沌并实现高速长距离混沌通信，有效抑制了光 混沌时间延迟特征[18] 。Li Mi 等人研究出增加一个复杂的可变射频放大器增益 密钥，便可以提高混沌光通信系统的安全性[19]。

1.3 图像加密研究现状

图像加密的过程分为置乱和扩散， 将明文图像转变成无法识别的样式，达 到保密的目的。将图像加密方法与其他算法相结合是近些年研究的主要方向，

比如混沌算法[20-25] 、DNA 序列编码算法[26-31]、椭圆曲线算法[32-37]、压缩感知算 法[38-43]等。Huang Wei 等人研究出了一种利用双图像进行压缩加密的算法。所 提出的方案涉及对两幅图像小波变换获得的稀疏矩阵进行置乱和压缩，最终的 类噪声密码图像是通过将密文图像的一半映射到另一半密文图像的 Alpha 通道 中来产生的[44] 。Wang Xingyuan 等人给出了一种使用混沌测量矩阵和随机相位 掩模的彩色图像加密算法。算法中利用切比雪夫混沌序列生成翻转置换矩阵、

采样子集和混沌循环矩阵，用于构造结构感知矩阵和随机相位掩模。 利用压缩 感知对初始图像同时压缩和加密，并且使用二维分数傅立叶变换重新加密[45]。

Xie Yiyuan 等人提出了一种利用光学混沌和半导体激光器的新型图像加密系统， 利用主激光器注入相同的混沌，附属激光器（SL1 和 SL2）可以输出相似的混 沌信号作为混沌载体来传输图像。同时，SL1 的混沌信号可用于生成加密方案 的密钥。采用三维（3D）猫图和逻辑混沌图打乱图像像素的位置，同时混淆了 密文图像和明文图像之间的关系[46] 。Li Lili 等人研究出了一个新颖的图像加密 和方案，并使用了光学中的混沌现象。 通过对主激光器进行光学反馈和注入，

从激光器可以生成混沌信号，采用 Logistic 混沌映射改变明文图像的像素位置 和值来增强彩色图像加密的安全性[47] 。Dong Wenglong 等人研究了一种使用多 光学混沌和像素值伪随机替换的彩色图像 DNA 加密系统，在激光混沌系统中 使用随机子块置乱和 DNA 序列编码，生成复杂的混沌序列进行加密和传输， 实现图像洗牌和扩散[48] 。Liang Qin 等人提出了一种新型的一维正余弦混沌映射 ( SCCM )，证明了 SCCM 比现有更先进的一维混沌映射具有更好的混沌性能， 还介绍了使用 SCCM 以及随机 DNA 操作的图像加密算法[49] 。Wang Xingyuan

3

中国知网 https:Www.cnki . net

等研究人员提出了一种创新型图像加密算法， 该算法巧妙融合了多目标粒子群 优化策略、DNA 编码技术和一维 Logistic 混沌映射。该方案采取了一种创新的 方法，通过运用 Logistic 混沌映射和 DNA 编码技术来生成用于混淆图像的随机 DNA 掩码。接下来，将此 DNA 掩码与经过分块打乱处理的明文图像 DNA 编码 序列相结合，共同构成了一个完整的图像加密系统。在 PSO 中,一个粒子的位置 值表示一副明文图像,循环 PSO 优化基于图像熵和相邻像素相关性。最终，在整 个过程中获取到最优密文结果后，将此刻对应的最佳粒子状态值反馈回来[50]。

融入 DNA 序列编码的图像加密算法由于能够有效抵挡选择明文攻击且计算 难度不高，近年来受到广泛关注。 Zhan Kun 等人提出利用四维超混沌系统和 DNA 编解码相结合的图像加密方案。加密过程涉及将图像强度值转换为二进制 流并使用超混沌序列对其进行加扰，DNA 序列运算用于增强加密性能[51]。 Zefreh 研究了利用 DNA 计算、混沌系统和哈希函数的新的图像加密方案，方案 包括 DNA 水平排列和扩散以实现高效率[52]。

混沌系统也广泛用于图像加密，因为混沌具有一些理想的密码学特性，例 如确定性系统中的初始值敏感性和不规则的内部随机运动。运用混沌映射的图 像像素扰乱方法受到许多学者的喜爱。Wu Xiaolin 等人在对纯基于混沌帐篷映 射方案的安全性分析的基础上，结合矩形变换和 CTM 原理，提出了一种新颖 的图像加密算法。它对明文图像的三个通道都加密，并且使得这些通道相互关 联。另外，通过将密钥和明文图像相关联，其密钥敏感性得到了进一步增强[53]。 Xue Hanwen 等人研究了一种用在彩色图像感兴趣区域( ROI )的超混沌加密算法， 该方案具有三个正李亚普诺夫指数和分层密钥的新型超混沌系统来确保安全性 [54]。

几种常见的混沌映射方案如逻辑映射、帐篷映射、正弦映射、超混沌映射 等。除了传统的混沌映射图像加密之外，光学混沌也普遍运用在图像加密上面。 Wang Anbang 等人展示了通过连续波光注入来加强激光器产生的混沌信号的带 宽，并且利用具有光反馈的分布式反馈半导体激光器作为混沌激光器。结果表 明，与没有光注入时观察到的带宽相比，当对混沌激光器应用光注入时，混沌 信号的带宽增强了大约三倍[55]。

1.4 论文的主要工作与结构

本文结合激光器动力学和图像加密算法， 提出了新型的基于激光混沌的 DNA 图像加密算法，以及将多目标粒子群优化算法运用至图像加密中，加强了 安全。

4

中国知网 https:Www.cnki . net

1.4.1 论文主要研究内容

（1）一种运用 Lorenz 超混沌和循环 DNA 序列编解码的图像加密方案

本方案的加密过程主要包括两步： 置乱和扩散。在图像置乱阶段，图像被 转化为比特信息流，然后论文提出了 LTM (Logistic-Tent Map) 混沌映射，通过 结合 LTM 混沌与 Fisher-Yates 洗牌算法，对比特流数据进行重新排序并重构图 像。

在扩散阶段，Lorenz 超混沌将被融入 DNA 编码过程中。采用 Lorenz 超混 沌系统的随机输出与原始图像像素值进行特定运算，或者根据这些高度随机序 列制定并应用到图像像素上的 DNA 编码策略，进而对已经过块级扰动处理的 图像实施逐像素、循环式的 DNA 加密过程，从而最终生成安全的加密图像。

该加密系统的密钥由两部分组成： 一是通过对给定图像的哈希序列进行特 定运算得到的值，二是用户可以自主设定的一个值。这两个密钥将介入之后的 混沌产生。经过多轮仿真和安全性测试， 论文证明了此加密系统具有较高的保 密性和优秀的加密性能。

（2）一种结合光混沌置乱、DNA 扩散和多目标粒子群优化算法的图像加密方 案

本方案采用主激光器（ML）发射激光至两对附属激光器（TPSL）产生两对 同步的混沌信号，并将激光混沌序列转换到灰度图像的阶别 0-255 之内，以便 进行后续的加密操作。加密过程有三个主要部分：密钥生成、置乱和 DNA 编 码扩散。

在密钥生成阶段，通过 SHA-384 算法算出输入图像的散列值，并通过多目 标粒子群算法优化得到优化值。在置乱阶段，上一步骤两个值进行异或运算， 得到的值用于调制 ML 的偏置电流，从而驱动 TPSL 生成两对同步混沌序列。 这些序列通过特定算法与初始图像的哈希值结合，生成两个密钥。接着，通过 使用这两个密钥将图像的像素位置打乱，并运用 DNA 编码将图像像素扩散。

此外，本系统运用多目标粒子群算法来优化加密过程。 系统将所有得到的 加密图像视为整个群体，每个粒子对应一个加密后的图像。优化的目标是最大 化密文图像的熵并且最小化密文图像像素之间的相关性。然后， 系统将帕累托 主导粒子选出来放入存储库中，并通过循环获取最佳粒子群位置，用于调制 ML 的偏置电流。

在接收端，通过与发送端的激光同步，便可以得到两个与发送端相同的密 钥。在这里，系统使用这两个密钥进行反向扩散和解密操作， 以还原初始图像。 通过对该方案算法的一系列安全性测试，结果表明该方案所提出的加密算法具

5

中国知网 https:Www.cnki . net

有良好的保密性。

1.4.2 论文的结构安排

论文的结构如图 1.1 所示。

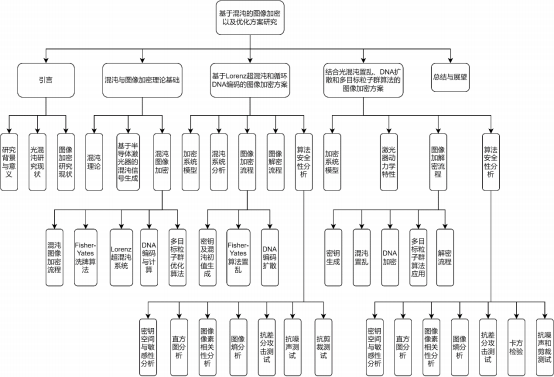


图 1.1 论文结构图

第一章基本讲了此研究的背景和意义，阐述了激光器动力学行为和图像加 密的研究现状，最后规划了本文的内容框架，对每个章节进行了简短的描述。

在第二章节中，阐述了混沌理论的基本原理，并详述了如何通过诸如光反 馈机制、光注入技术和光电混合反馈等方式， 在半导体激光器系统中生成混沌 信号。之后说明了图像的加密过程，介绍了本论文中出现的加密方法。

第三章研究了采用 Lorenz 超混沌系统和循环 DNA 编解码的图像加密算法。

算法结合了 Lorenz 超混沌、Fisher-Yates 洗牌算法以及 DNA 编解码。将图像经 过洗牌置乱后再进行循环 DNA 加密来得到加密图像。并对密文图像进行测试， 证明此算法的健壮性。

第四章介绍了一种结合光混沌扰乱、DNA 扩散和多目标粒子群优化算法的 图像加密方案。该方案使用光混沌与索引排序将图像像素扰乱，之后用 DNA 编码算法将图像像素值扩散，将每次加密获得的图像都作为粒子群的粒子进行 一定次数的迭代，从而得到具有最佳适应度的粒子（即密文图像）。然后测试了

6

中国知网 https:Www.cnki . net

此加密方案的安全性，结果说明方案的保密性较高。

第五章对本文的工作内容进行了总结，通过总结阐述了目前存在着哪些问 题，并对以后的工作方向和改进内容作了一定程度的展望。

7

中国知网 https:Www.cnki . net

第二章 混沌与图像加密理论基础

本章主要介绍课题相关理论基础和关键技术，主要论述了混沌、激光器混 沌、混沌图像加密的理论基础，以及对课题使用的技术进行了介绍。

2.1 混沌理论

混沌是独特的自然现象，它表现出无规则的和伪随机的行为，但是又产生 于确定性系统中。混沌的这种行为具有高度的不可预测性和不确定性，既没有 明显的周期性，也不会收敛到某个固定状态。混沌并不是纯粹的无序或随机， 而是一种复杂的、非线性的存在形式，其中包含着充足的内部有序构造。

混沌系统的整体行为是确定的，具有稳定性，但是其局部行为却是不稳定 的。这归因于混沌系统的行为对初始条件很敏感，初始条件中微小的改变都会 造成系统运动轨迹的难以估量的偏离。之后这种偏离会不断放大， 导致混沌系 统的未来状态更加难以预测。

混沌理论在许多领域都有应用价值，例如气象预测、经济学、生物学等。

通过理解混沌现象，人们可以更好地理解自然界的复杂性和非线性系统的行为， 从而在科学、工程和日常生活中做出更准确的预测和决策。

2.1.1 混沌系统的定义

Li-Yorke 对混沌的定义为[56]：对于区间 L 上的连续自映射 f(x)，判断是否满 足下列条件，

（1） f 的周期点的周期无上界。

（2） 闭区间 L 上存在不可数子集 P，满足：

(ⅰ)对任意 *x*, *y*∈*P*，当 x≠y 时，有

lim sup *f* *n*(*x*)− *f n*(*y* ) > 0 (2.1)

n →∞

(ⅱ)对任意 *x*, *y*∈*P*，有

 (2.2)

(ⅲ)对任意 x∈P 和 f(x)的任一周期点 y，有

lim sup *f* *n*(*x*)− *f n*(*y* ) > 0 (2.3)

n →∞

那么，f(x)在不可数子集 P 上是混沌的。

8

中国知网 https:Www.cnki . net

2.1.2 混沌的性质

混沌系统的非线性动力学特性主要有以下几点：

（1）内在随机性：混沌系统在确定的非线性动态系统中产生伪随机的运动， 其轨道难以预测。

（2）敏感依赖性：对于初值，即使是很小的变化也会造成长期行为的大不 同。

（3）奇异吸引子：混沌系统具有奇异吸引子，它是一种复杂且不规则的几 何形状，可以捕获系统状态的运动并吸引所有附近的轨迹。

（4）分形结构：混沌系统的轨道常常在空间中形成复杂的分形结构。

（5） 自相似性：混沌系统的某些特征具有自相似性，即在不同尺度上重复 出现相同或相似的模式。

（6）普适性：不同混沌系统的某些动力学特性在某种程度上是类似的，这 种类似性称为普适性。

（7）长期不可预测性：由于混沌系统的内在随机性和对初始条件的敏感性， 使得对长期行为的预测变得不可能。

系统的非线性虽然是产生混沌行为的前提条件，可这并不是唯一决定因素。 一个系统是否真正存在混沌行为，通常需要算出其混沌系统的李雅普诺夫指数 来确认。

李雅普诺夫指数是一种衡量系统动态行为稳定性的工具[57]。在一个可能具 有混沌特性的系统中， 如果存在正的李雅普诺夫指数，那么这通常是系统呈现 混沌行为的重要证据。这是因为正的李雅普诺夫指数表明系统的相邻轨迹在相 空间中会以指数速度发散，这正是混沌系统对初始条件极度敏感的特性之一。 以一维混沌映射为例分析李雅普诺夫指数，如公式(2.4)所示，它只能在某一个 方向上拉伸或压缩。

*xn*+1 = *f* (*xn* ) (2.4)

在公式(2.4)中，设置初值 x0及它的相近值 x0+δx，迭代一次 f(x)后，它们之间的 间距是*δx*1 = *f* (*x*0 + *δx*) − *f* (*x*0 ) ≈ *f* ′ (*x*0 )*δx* ，经过 n 次迭代后出现指数分离现象，

这个过程如公式(2.5)所示：



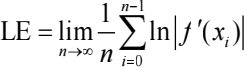


(2.5)

则可以推出李雅普诺夫指数的数学定义是：

9

中国知网 https:Www.cnki . net

 (2.6)

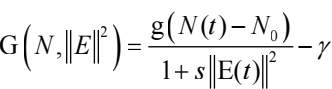
当 Lyapunov 指数（LE）大于 0 时，系统的局部稳定性丧失，相邻的轨道会以 指数速度迅速分离，这会导致混沌吸引子的形成，标志着系统进入混沌状态。 而在 Lyapunov 指数等于 0 的情况下，系统的运动轨道表现出稳定性，初始的误 差不会发生变化。当 Lyapunov 指数小于 0 时，系统的运动轨迹在局部范围内保 持稳定，基本不受初值影响，且周期性的运动轨道比较稳定。

2.2 基于半导体激光器的混沌信号生成

半导体激光器 (SL)由于其构造简洁、成本低廉的表征，被认为是生成光混 沌的理想选择，并因此成为了研究的重点。以下将详细介绍半导体激光器产生 混沌信号的几种方法及其相关的理论基础。

对半导体激光器增加一个自由度使其产生混沌，方法主要有光反馈、光注 入以及光电反馈。根据 Kobayashi 和 Lang 于 1980 年共同提出的半导体激光器 动力学理论框架，半导体激光器（SL）的内在动力学系统可借助描述场振幅变 化率和载流子密度变化率的方程式来表示：

 (2.7) 

 (2.9)

其中 E 表示光子数， N 表示载流子数， ||E||2 表示 SL 的慢变电场振幅，

G(*N*, *E* ) 为增益函数，e 为电荷电量，α 为线宽增强因子，I 表示偏置电流，g 为差分增益系数，s 为增益饱和系数。*γ* 为光子衰减速率，*γ*e 为载流子复合速率。

2

（1）基于光注入的混沌

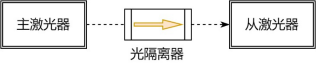


图2.1基于光注入的混沌生成

在图 2.1 中，本节展示了一个采用光注入技术的半导体激光器系统。在这个 系统中，ML 产生的相干光场通过光隔离器，单向地注入到附属激光器内。当

10

中国知网 https:Www.cnki . net

ML 和 SL 之间的频率差和光注入强度达到特定要求时，SL 的稳态行为将会被 干扰。在这时，我们便能够在 SL 的输出光中观察到混沌现象。ML 和 SL 的慢 变复光场可以表示为：

 (2.10)

*Es* + *kEM* *τ e*−*i*Δ (2.11)

其中，EM和Es分别代表 ML和 SL各自的慢变光场振幅。参数k体现的是注入光 的强度效应，而τ则定义了注入过程中的时间延迟。ML的工作频率记为 ωM，且 Δω代表 ML和 SL之间的频率间隔。通过对注入光强度、相位的精细调控，或是 增加主从激光器间的频率差异，能够促使从激光器从稳定的运作状态逐渐转变 至混沌状态。

（2）基于光反馈的混沌

下面的系统架构图描绘了用于实现高维混沌光学输出的基础装置，该装置 是集成了光反馈机制的单模半导体激光器，它构成了此类信号产生的核心硬件

配置。

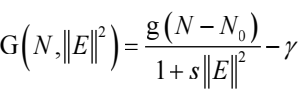


图2.2 基于光反馈的混沌生成

该反馈机制是由激光器输出的一部分经过外部反射镜反射并引入一定时间 延迟后，重新返回到激光器的谐振腔内形成的。混沌现象的产生源于反射光与 激光器内部的弛豫振荡之间的相互作用。动力学方程如下：

*E* + *kE* (2.12)

 −*γeN* −  (2.13)

 (2.14)

在该方程中，光反馈效应由*kE*(*t* −*τ*)*e*−*iω*0*τ* 来代表，其中反馈强度记为k，而反馈 时滞则为τ。当采用相位共轭镜（PCM）替代传统外部光反馈结构中的平面反射 镜时，激光在从激光器传播至PCM阶段所累积的所有相位偏差与扩散效应，在 光束经过PCM反向传输回激光器的过程中均能得到精确抵消，进而确保整个外 腔循环过程中的净相位变化近乎于零[58][59]。这一改良后的配置能够有效地生成

11

中国知网 https:Www.cnki . net

具有更广泛频谱带宽的混沌信号。此种利用相位共轭技术实现激光混沌产生的 方法被称作相位共轭反馈（PCF）。

在应用相位共轭反馈机制时，考虑到实际操作中反馈元件总会存在一定量 的时滞，例如在反射器中的响应时间，但这会影响到系统的实时性。然而， 理 论上可以设想一种理想化的相位共轭镜（PCM），其响应时间趋近于零，并且 在反射光束时不引入任何额外的频率变化。在此理想化情境下，通过PCM实现 的激光器动力学行为可以用公式 (2.12) 来精确描述和推演：

*E* + *kE*\*  (2.15)

此理论框架与之前由式(2.7)所表述的一般光反馈在本质上有相近之处，不同之 处仅在于PCF（相位共轭反馈）条件下的速率方程中，反馈项的表达中，选取 了光场的复共轭量 E\* 进行应用。相较于传统的使用平面镜进行的常规光反馈 (COF)，相位共轭镜因其独特的自校正与自对准反馈属性而脱颖而出[60][61] ，其 结构使得经由PCM反射回来的相位共轭反馈光束能自动与入射到PCM上的激光 束保持对准。在这种情况下，PCF所需的反馈强度更高时就能引发混沌现象， 这意味着PCF体系具有更广泛的稳定性边界。并且，相位共轭反馈（PCF）还能 够激发更为复杂的非线性动力学反应，并在频谱平坦度及统计复杂性特征方面 显示出相较于传统光反馈（COF）更为卓越的表现。

（3）基于光电反馈的混沌

光电反馈作为一种引导半导体激光器进入混沌状态的技术手段，其运作机 制可概述如下：半导体激光器发射出的光信号首先进入一个高速响应的光电探 测器，该探测器负责将接收到的光信号转换为电信号形式。随后，该电信号通 过适当的电路进行一系列处理，包括延时、带通滤波和放大等步骤。经过处理 的电信号与激光器原有的偏置信号合并后，再将整合后的信号回送至激光器内 部进行反馈调节。这种反馈机制如图 2.3 所示。

12

中国知网 https:Www.cnki . net

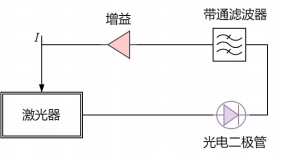


图 2.3 基于光电反馈的混沌生成

该方案是在激光器的偏置电流中引入循环反馈来产生混沌。这种反馈扰动 会导致激光器内部的载流子数量发生变化，进而引发混沌行为。

2.3 混沌图像加密

本节主要介绍混沌图像加密的理论，主要介绍加密过程以及在本文中出现 的图像加密方法的实现。

2.3.1 混沌图像加密流程

混沌图像加密的流程一般有这几步：

（1）预处理：将要加密的图像文件读入到程序中。如果需要，可以将图像从一 种颜色空间（比如 RGB）变到另一种更适合加密的颜色空间（如灰度或 HSV）。 （2）密钥生成：根据安全性和效率需求，选择一个合适的混沌系统，如 Lorenz 系统、Logistic 映射、Henon 映射等。运用自己设置的密钥或其他随机源来作为 混沌系统的初始条件和参数。然后迭代混沌系统，产生所需的混沌序列，这个 序列将用于后续的加密过程。

（3）扩散和混淆：将图像划分为多个像素区块逐一进行处理，或者选择逐像素 的方式来完成图像操作。对每个像素或像素块执行以下一种或多种操作，使用 混沌序列作为输入。根据混沌序列重新排列像素的位置，用混沌序列中的值替 换像素的亮度或颜色分量。

（4）加密图像生成：完成所有扩散和混淆操作后，得到的图像就是加密后的图 像。将其保存为一个新的文件，以备传输或存储。

（5）解密过程：使用相同的混沌系统、参数和密钥，重复上述过程，但执行逆 操作：首先，对加密图像进行与加密时相反的操作（如位置恢复、值替换和位 翻转）。然后，将图像转换回原始的颜色空间（如果在加密前进行了转换）。经

13

中国知网 https:Www.cnki . net

过解密恢复的图像应当看起来和原始图像高度相似。

（6）安全性评估和优化：对加密算法进行各种攻击测试，如差分攻击、已知明 文攻击等，以评估其安全性。根据测试结果和实际需求，调整混沌系统参数、 改进扩散和混淆方法，以及优化加密和解密的性能。

利用混沌的图像加密方案基本流程如图 2.4 所示：

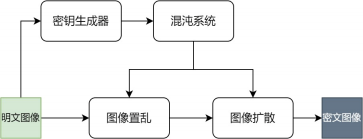


图 2.4 混沌图像加密流程

2.3.2 Fisher-Yates 洗牌算法

Fisher-Yates 洗牌算法也被称为 Knuth shuffle 或 Durstenfeld shuffle，是一种 用于随机打乱数组或列表元素顺序的算法。该算法确保每个元素都有相等的机 会出现在任何一个位置上，从而产生真正的随机排列。以下是 Fisher-Yates 洗牌 算法的基本步骤：设定一个要洗牌的数组 Data，包含 n 个元素。

（1）从最后一个元素（索引为 n-1）开始，遍历到第一个元素（索引为0）。

（2）对于当前索引 i，生成一个随机的整数j，满足 0 <= j <= i。

（3）将索引为 i 和j 的元素进行交换，即：将 Data[i]与 Data[j]的值互换。 继续这个过程，直到遍历到数组的第一个元素为止。

2.3.3 Lorenz 超混沌系统

超混沌系统可以弥补低维度混沌系统的局限性，进而生成更为错综复杂的 混沌序列。超混沌系统由于其轨道膨胀特性， 比传统的混沌系统更为复杂。它 们可以同时产生许多不同的伪随机序列， 能够让它们在加密应用中更加灵活和 安全。

Lorenz 混沌是指在研究大气对流现象时，由美国气象学家 Edward Lorenz 发 现的一种混沌行为[62] 。Lorenz 混沌是通过 Lorenz 系统来表述的，这是一个三维 非线性常微分方程组，最初是为了简化和模拟大气中温度、压力和风速之间的 复杂相互作用而提出的。Lorenz 系统的基本形式如下：

14

中国知网 https:Www.cnki . net

 (2.16)

 (2.17)

 = *xy* − *βz* (2.18)

其中，x 、y 和 z 是系统的三个状态变量，σ 、ρ 和 β 是系统参数。Lorenz 系统最 著名的特性是在特定参数值下（例如，σ = 10 ，ρ = 28 ，β = 8/3）表现出的混沌 行为。当 Lorenz 系统处于混沌状态时，其轨迹呈现出一种称为"蝴蝶效应"的敏 感依赖于初始条件的特性，即非常小的初始差异会随着时间的推移而迅速放大， 导致系统状态的大幅变化。

Lorenz 混沌不仅在气象学中有重要应用， 也在许多其他领域如物理学、生 物学、经济学以及密码学等领域中被广泛研究和应用，特别是在混沌领域和复 杂系统的研究中有着举足轻重的作用。

2.3.4 DNA 编码和计算

随着生物科学与计算机科学的交叉融合，又一崭新的热门学科领域正蓬勃 发展。如人工神经网络、遗传算法等技术正是生物学原理在计算范畴的成功应 用实例。尤其是在人类基因组计划完成及其后续研究阶段，生物分子数据呈现 出指数级增长态势，科学家们面临着如何有效提取并解读这些海量数据背后的 生命规律这一重大挑战。20 世纪 90 年代，Adleman 通过运用 DNA 分子技术开 展了一项创新性的生物化学实验，搞定了涉及 7 个顶点的有向哈密尔顿路径问 题。此举不仅证明了现代分子生物学方法可用于计算过程，也预示着可以通过 生物技术手段攻克极其复杂的组合优化难题。这一成就标志着计算科学研究领 域的一个崭新分支的诞生，并极大地促进了跨学科 DNA 计算技术的发展，其 意义深远重大。

DNA 密码学是一个在 DNA 计算技术启示下新兴的密码研究分支，核心特 点在于运用 DNA 分子作为信息存储和传输介质，并利用现代生物科学技术手 段来实现密码操作。这一领域充分利用了 DNA 内在所具备的高度并行处理能 力、卓越的储存密度以及极低的能量消耗特性，以达成密码学的安全功能与目 标。DNA 计算的基础理念是利用 DNA 分子作为信息载体，通过精心设计的反 应过程对信息进行处理和运算。在这个模型中，计算过程实质上就是 DNA 分 子状态的转换，初始状态下编码的数据信息经由一系列计算被转化和操作，最 终得到的新 DNA 分子状态则被视为计算得出的结果。

15

中国知网 https:Www.cnki . net

DNA 作为一种双链聚合物，其独特的结构特征是呈双螺旋形态。 有四种含 氮碱基，包括腺嘌呤（A）、胸腺嘧啶（T）、鸟嘌呤（G）和胞嘧啶（C）。其中， A 与 T 、G 与 C 分别为互补关系。在灰度图像中，单个像素点的亮度信息通常 采用 8 位二进制数来精确描述和存储，四个脱氧核苷酸 A 、T 、C 、G 可以表示 两个二进制位（例如 00 、01 、10 、11），则灰度图像中的每个像素都可以转换 为四位 DNA 序列。例如， 218（11011010）可以表示为 DNA 序列 GTCC。

DNA 分子的核苷酸可编码成 8 条规则，如表 2.1 所示。

表 2.1 DNA 编码规则

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 规则 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 00 | A | A | C | C | G | G | T | T |
| 01 | C | G | A | T | A | T | C | G |
| 10 | G | C | T | A | T | A | G | C |
| 11 | T | T | G | G | C | C | A | A |

本文研究使用的 DNA 操作有 DNA 加减法和异或运算，其中DNA 核苷酸之 间的运算与二进制之间的运算类似。使用规则 1（A-00 、G-10 、C-01 、T-11） 作为编码原则的示例如下表 2.2-2.4 所示：

表 2.2 DNA 加法运算

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 加法 | A | G | C | T |
| A | A | G | C | T |
| G | G | A | T | C |
| C | C | T | G | A |
| T | T | C | A | G |

表 2.3 DNA 减法运算

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 减法 | A | G | C | T |
| A | A | G | T | C |
| G | G | A | C | T |
| C | C | T | A | G |
| T | T | C | G | A |

表 2.4 DNA 异或运算

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 异或 | A | G | C | T |
| A | A | G | C | T |
| G | G | A | T | C |
| C | C | T | A | G |
| T | T | C | G | A |

2.3.5 多目标粒子群优化算法

群智能优化算法是专家学者通过对一些自然现象或者生物觅食、筑巢等行

为特征的观察模仿，提出的许多高效的优化算法，如模拟退火算法、遗传算法 [63]、蚁群算法[64] 、粒子群算法[65][66]、细菌觅食算法、人工蜂群算法等。将优化 算法用在图像加密中，选择适当的适应度函数来优化生成密文图像的信息属性， 例如信息熵和像素相关性，可使加密效果非常接近理想值，更好的抵抗熵攻击 和统计分析攻击。

1995 年，Kennedy 和 Eberhart 最初发表了粒子群的优化策略[67] 。粒子群优 化（PSO）算法是一种借鉴自然界中鸟类群居行为的集体智能搜索策略，它建 立在群体协同探索的基础上，通过模拟个体间的信息交流和位置更新机制，实 现对问题解空间的有效搜索。在 PSO 算法中，解决问题的过程被抽象为一群 “粒子”在解空间中的搜索过程。每个粒子代表一个可能的解决方案，并且都有 两个动态属性：速度和位置。所有粒子使用预设的适应度函数来衡量当前位置 的优劣，并以适应度值作为标准选择个体最佳位置、群体最佳位置和最佳个体 适应度值。因此，经过多次迭代后， 系统便可以找到最优解。优化步骤如下。

（1）初始化阶段：首先，在解空间中随机初始化一组粒子，每个粒子的位置表 示一种潜在解，速度决定该粒子在解空间中移动的快慢和方向。

（2）评估阶段：计算每个粒子所对应位置的目标函数值（适应度），目标是找 到使目标函数达到最小（或最大）值的最优解。

（3）迭代更新：

（i）每个粒子记住自己曾经经历过的最佳位置，即个体极值（*Pbest*）。

（i）整个种群共享的信息包括所有粒子中找到的全局最优位置，即全局极 值（*Gbest*）。

(ⅲ)在每一次迭代中，每个粒子根据自身的个体极值、全局极值以及其当 前速度，通过预设的公式调整自己的速度和位置，向更好的解靠近。种群 迭代的速度和位置更新可表示为：

|  |  |
| --- | --- |
| *vi* (*t* + 1) = *ω* . *vi* (*t*) + *c*1*r*1 . (*Pbesti* (*t*) − *xi* (*t*))  + *c*2 *r*2 . (*Gbesti* (*t*) − *xi* (*t*)) | (2. 19) |
| *xi* (*t* + 1) = *xi* (*t*) + *vi* (*t* + 1) | (2.20) |

其中 vi(t)表示运动速度，xi(t)代表运动位置方向，*ω* 是惯性权重，r1 ，r2∈[0,1] 是随机向量，c1 ，c2 是学习因子，为常数。更新迭代的速度和位置通常有限制。 （4）收敛判断：算法经过多次迭代后，若满足停止准则（如达到预设的最大迭 代次数或全局最优解的变化小于阈值），则结束搜索；否则继续迭代。

多目标粒子群优化算法（MOPSO）是对标准粒子群优化（PSO）算法的一 种延伸，旨在应对同时优化多个目标函数的复杂场景。传统的单目标优化问题

17

中国知网 https:Www.cnki . net

是寻找一个单一目标函数的全局最优解，而在实际应用中，很多情况下会遇到 多个相互冲突的目标需要同时优化的问题，比如设计产品时既要降低成本又要 提高性能。

在 MOPSO 中，每个粒子不仅有一个位置向量，而且对应着多个目标函数 值。由于可能存在多个解无法通过单一标准比较优劣（因为优化不同的目标可 能会导致解决方案之间的权衡），因此不再追求单一的全局最优解，而是寻求非 支配解集（Pareto Optimal Set），即在所有解中找不到一个解能在不损害其他至 少一个目标的情况下改进所有目标。

在多目标优化算法中，多个目标不可能同时达到最优状态，只能尽量使多 个目标达到一种权衡最优状态。一个解 a 是帕累托最优当且仅当不存在比它更 好的解时，所有帕累托最优解的集合称为帕累托最优集。相应的目标向量称为 帕累托前沿[68]。帕累托优势决定了当前粒子适应度值是否优于历史适应度来选 择最优解。

MOPSO 的基本流程如下：

（1）初始化：创建一组粒子，并随机赋予它们初始的位置和速度。

（2）评估：计算每个粒子所对应位置的多个目标函数值，形成一个多目标适应 度向量。

（3）非支配排序与存储：根据非支配关系对粒子进行排序，并将非支配解存储 在一个称为外部档案（或称为 Pareto 前沿）的集合中。

（4）更新个体极值与全局极值：每个粒子更新其个人历史最优位置（pBest）， 同时整个种群共享并更新全局非支配前沿（gBest）。

（5）更新粒子状态：根据 pBest 、gBest 以及其他策略（如拥挤距离等避免过度 集中于某一片区域的策略）更新粒子的速度和位置。

（6）终止条件判断：迭代次数达到预设值或者满足某种收敛准则后停止搜索， 否则继续迭代。

通过上述过程，MOPSO 可以在多目标优化问题中找到一系列的帕累托最优 解，这些解为决策者提供了多种平衡不同目标之间冲突的可能选择。

2.4 本章小结

本章介绍了混沌图像加密的理论基础和相关加密手段。首先说明了混沌的 概念和定义，并介绍了混沌的性质和如何判断混沌。第二，介绍了半导体激光 器生成混沌的方法，如光注入、光反馈和光电反馈，并给出了相应的模型以及 动力学方程。第三介绍了混沌图像加密的基本流程，并介绍了置乱和扩散中使

18

中国知网 https:Www.cnki . net

用的加密方法，如 Fisher-Yates 算法，DNA 序列编码。第四引入了粒子群优化 算法，并列出了粒子群算法的执行步骤。

19

中国知网 https:Www.cnki . net

第三章 基于 Lorenz 超混沌和循环 DNA 编码的图像加密方 案

本章节提出了一种综合运用 Fisher-Yates 随机置乱算法、DNA 编码技术以及 超混沌 Lorenz 系统的图像加密方案。该方案首先通过计算待加密明文图像的哈 希值以生成加密密钥，此密钥进而被用作混沌系统初始化的输入参数。在加密 过程中，先运用 Logistic-Tent 混沌映射（LTM）与 Fisher-Yates 算法相结合的方 式对原始图像进行打乱处理；紧接着，超混沌 Lorenz 系统产生混沌序列，这一 序列作为掩模应用于 DNA 编码及其后续的操作步骤。最后，通过对已置乱图 像块应用基于 DNA 扩散的加密技术，从而生成最终的密文图像。经过实验验 证和一系列安全性分析，该方案展现出卓越的加密性能，并能有效抵御多种常 见的密码攻击手段。

3.1 加密系统模型

系统的加密流程如图 3.1 所示。首先，通过哈希算法算出明文图像的散列值， 将该序列值与给定的值进行运算后再作为混沌系统的初始参数以及整个加密系 统的密钥。接下来，将基于此密钥生成的混沌序列与加密系统深度融合：这个 加密系统具体涵盖了 Fisher-Yates 随机置乱算法和 DNA 循环编码扩散机制。经 过这两个关键步骤后，即可完成对原始图像的加密处理并得到加密图像。

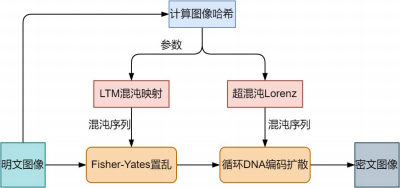


图 3.1 系统流程图

3.2 混沌系统分析

本章提出了耦合混沌映射 Logistic-Tent Map（LTM）的概念，耦合混沌映射 20

中国知网 https:Www.cnki . net



是由逻辑映射和帐篷映射结合而来。方程如下。

*F*(*xn*+1) = mod(*f* (*xn* ) + *g*(*xn* ),1) (3.1)

f(xn) 和 g(xn)是两个不同的一维混沌映射，mod(x,y)是模运算，返回 x 除以 y 的 余数，耦合混沌的范围在 0-1 之间。

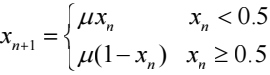
LTM 是由 Logistic 映射和 Tent 映射耦合而来，这两种一维混沌映射使用较

为广泛，方程分别为：

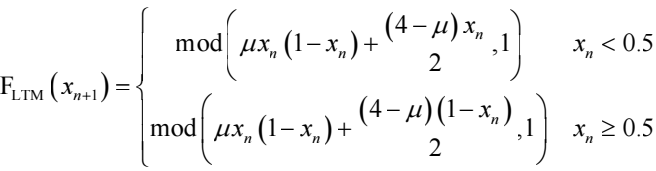
*xn*+1 = *μxn* (1− *xn* )

(3.2)

(3.3)

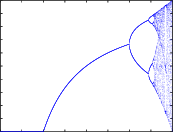
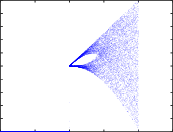


耦合逻辑-帐篷映射（LTM）表示为：



(3.4)

其中 *μ* ∈(0, 4] ，Logistic 映射、Tent 映射、LTM 的分岔图如图 3.2 所示。LTM 的 输出在 (0, 4] 中分布比较均匀，其范围大于逻辑映射和帐篷映射。

1

1

0.9

0.9

0.8

0.8

0.7

0.7

0.6

0.6

0.5

x(n) x(n)

x(n)

0.5

0.4

0.4

0.3

0.3

0.2

0.2

0.1

0.1

0

0

1.5 2 2.5

2

μ

(b)

0 0.5 1

0

0.5

1

1.5

2.5

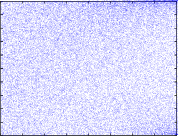
3

3.5

4

μ

(a)

1

0.9

0.8

0.7

0.6

0.5

0.4

0.3

0.2

0.1

0

2 2.5 3 3.5 4

0 0.5 1 1.5

μ

(c)

图 3.2 混沌分岔图。（a）Tent 映射；（b）Logistic 映射；（c）LTM

21

在本系统方案中，根据公式(2.16)-(2.18) ，Lorenz 超混沌的参数设置为 σ = 10 ，ρ = 28 ，β = 8/3 ，而初始值则由密钥决定。Lorenz 超混沌的吸引子如图所示。

|  |  |  |  |
| --- | --- | --- | --- |
| y | 30  20  10  0  -10  -20  -30 | |  | | --- | |  | |

-20 -15 -10 -5 0 5 10 15 20

x

50

|  |
| --- |
|  |

45

40

35

30

25

20

15

10

5

0

-20 -15 -10 -5 0 5 10 15 20

x

50

(a)

45

|  |
| --- |
|  |

40

35

30

25

20

15

10

5

0

0

-20

-10

-30

10

20

30

y

(c)

(b)

50

40

30

20

10

0

40

20

20

10

0

0

-10

-20

-20

y

x

(d)

图 3.3 洛伦兹超混沌吸引子。（a）x-y 相空间；（b） x-z 相空间；（c） y-z 相空间；（d） x-y- z 相空间。

3.3 图像加密流程

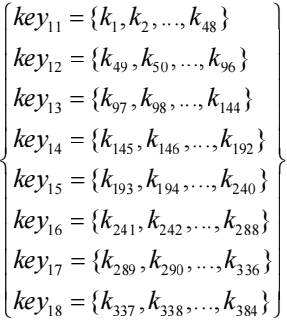
本加密方案包括密钥生成、Fisher-Yates 算法置乱和 DNA 扩散三个步骤。具 体流程将在以下小节介绍。

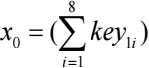
3.3.1 密钥以及混沌初始值生成

依照式(3.5)所示，首先运用 SHA-384 哈希算法对原始图像进行运算，生成 对应的哈希值，随后将这个十六进制格式的哈希值进一步转化为一个由 384 位 二进制数字构成的密钥 key。将密钥每 48 位分成一组，将每一组二进制转换成 十进制大数，通过依次相加之后再经过式(3.7)运算得到 LTM 混沌初值。散列算 法的优点就在于密钥与明文密切相关，所以当明文图像发生变化时所计算出的 哈希值也将不同。

*key* = {*k*1, *k*2, *k*3,..., *k*384 } (3.5)

22

*key* =  (3.6)

 .10−12 (3.7)

把 key1i 依次异或后所得的比特序列换算成十进制数字 b。再通过式(3.8)映射， 作为 Lorenz 超混沌的初值。

*m* = −20 + mod(*b*, 40) (3.8)

其中 mod()函数为取模。其目的是将 Lorenz 超混沌的初值范围限制在-20 到 20 之间。LTM 混沌的 μ 值将由加密人员给定，作为一个密钥， *μ* ∈(0, 4]，同时它 也作为 Lorenz 超混沌的其中一个初值。

3.3.2 Fisher-Yates 算法置乱

步骤 1：将图像信息转变成比特流序列 V。

步骤 2：利用密钥和 LTM 混沌产生与比特流长短 n 相等的混沌序列 S 。 步骤 3 ：从比特序列的最后一个元素开始循环，并依次减小 1 ，i=n→ 1。

步骤 4：利用混沌序列 S 生成随机下标 j，如式(3.9)所示。其中 ceil()函数表 示向下取整。

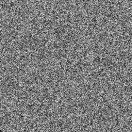
*j* = *ceil*(*i* . *S*(*i*)) (3.9)

步骤 5：交换 V(i)和 V(j)。

经过混沌与 Fisher-Yates 算法结合置乱后的图像 P 如图所示。

23

中国知网 https:Www.cnki . net



(a) (b)

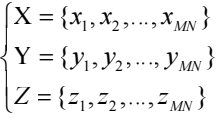
图 3.4 图像像素置乱。(a)原始图像；(b)置乱后图像。

3.3.3 DNA 编码扩散机制

步骤 1：将两个密钥输入到超混沌 Lorenz 系统中，参数设置为 σ=10 、ρ=28、 β=8/3，密钥形成的系统的初始值 u0为：

*u*0 = [*μ*,1, *m*]T (3. 10)

假设图像大小为 M×N，系统生成 10000+M×N 长度的伪随机序列，并丢弃前 10000 个值以获得更好的随机效果，得到 M×N 长度的混沌序列 X ，Y ，Z。

 (3. 11)

步骤 2：将 X 序列映射到 0-255 内，并将其重塑为 M\*N 大小的矩阵。如式 (3.12)所示。其中，*i* ∈[1, *MN*] ，floor(•) 是向下取整操作，reshape() 函数将序列 L 重塑成 M×N 矩阵 R，用于下一步 DNA 操作。

*Li* = mod(floor(*xi* × 108 ), 256) (3. 12)

*R* = reshape(*L*, *M* , *N*) (3. 13)

步骤 3：将置乱后的图像分成块，以提高 DNA 编解码的速度，并将图像矩 阵和扩散矩阵 R 都分为 4×4 的小矩阵。DNA 编码和解码的方式由以下公式确定。

*k*1*i* = mod(*Li* ,8) +1 (3. 14)

其中 k1i 决定了图像和扩散矩阵各块的编码方式，可以表示数字 1 到 8，分 别代表 DNA 的 8 种编码规则。

*k*2*i* = mod(round(*yi* × 104 ), 4) (3. 15)

其中 k2i 控制了图像矩阵和扩散矩阵之间的 DNA 运算规则。它可以表示数 字 0-3，分别表示运算规则中的加法、减法、异或和同或。

24

中国知网 https:Www.cnki . net

*k*3*i* = mod(round(*zi* × 104 ),8) +1 (3. 16)

其中 k3i 决定了计算矩阵的解码规则。其中 mod(·)表示取模运算，round()函 数代表就近取整。DNA 扩散过程如图 4 所示。

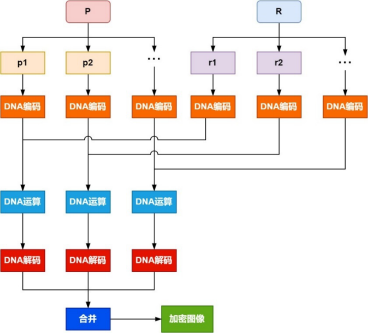


图 3.5 DNA 分块扩散过程

将置乱矩阵 P 和矩阵 R 分成块矩阵之后，依次进行 DNA 编码以及运算，再 将运算后的结果进行 DNA 解码，所获的图像像素值与原始图像将完全不相同。 合并后即可获得加密图像。

步骤 4 ：将步骤 3 循环 9 次运算，即可得到更加难以预测的加密图像。

3.4 图像解密过程

图像解密是加密的逆过程，本方案采用对称加密方式， 只有获得加密密钥 才能进行以下解密过程。

输入：密文图像 C ，密钥序列 key ，Lorenz 超混沌初值 m ，μ。

步骤 1：首先进行 DNA 循环逆扩散，过程与加密时是相同的。解密的耗时 如下表所示，由表中数据可得解密耗时较短， 效率较高，具体耗时差异还与实 验所用机器性能有关。

表 3.1 所提出方案的图像解密时间

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 图像 (256×256) | 鹦鹉 | 蝴蝶 | 房顶 | 摄影人 |
| 解密耗时 (s) | 0.8134 | 0.8127 | 0.8343 | 0.8643 |

25

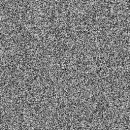
中国知网 https:Www.cnki . net

步骤 2：将逆扩散后的图像转换成比特序列，通过密钥得到 LTM 混沌序列， 用逆 Fisher-Yates 混淆运算两个序列，逆运算与加密时相反，即从前往后交换序 列值。

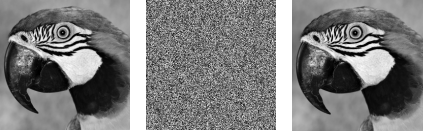
输出：明文图像。

3.5 算法安全性分析

本节将所论述的算法做了实验并分析，验证了方案的有效加密能力。本节 对一些 256×256 像素大小的图像进行了实验，结果如图 3.6 所示。从左到右依 次排列的是未经处理的原始图像、基于原始图像生成的加密图像，以及对所述 加密图像成功还原得到的解密图像。从图中可以看出，加密后的图像完全不可 辨认，无法从中获取有效信息，并且通过正确的密钥能将密文图像解密，这也 说明此算法的有效性。



(a) (b) (c)

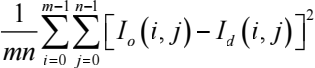


(d) (e) (f)

图 3.6 图像加解密结果。(a)和(d)是原始图像；(b)和(e)加密图像；(c)和(f)是解密图像。

除了观察法，我们还可以计算解密后的图片与原图的像素误差分布来证明

图像被完整的解密还原。通常可使用均方误差（Mean Squared Error, MSE）来 描述原始图像与解密后图像之间像素点的差异，均方误差是各像素差值平方的 平均值，公式为：

*MSE* =  (3.17)

其中 *I*o 和 *I*d 分别代表原图和解密后的图像，m 和 n 是图像的宽度和高度。通过 26

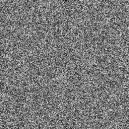
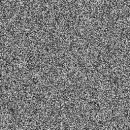
中国知网 https:Www.cnki . net

计算得到所有测试图像的原图与解密图像的均方误差都为 0，说明两幅图像毫 无差异。

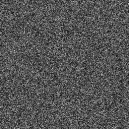
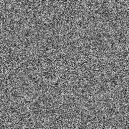
3.5.1 密钥空间与敏感性分析

密钥空间指的是加密密钥的数量以及加密密钥的大小， 密钥空间大小与系 统保密程度成正相关。一般来说，密钥空间需要大于 2100 才能抵挡暴力穷举法 的攻击[69]。在加密系统中，加密密钥有两个，一个是 384bit 的二进制数据，一 个是 0 到 4 范围的实数，实测敏感性能达到 10-15。所以系统的密钥空间大小为 2384 ×10-15，其值远远大于 2100 ，因此该算法拥有很强的安全性。

密钥敏感性是指密钥很小的变更将会造成大不相同的加解密结果。在系统 仿真实验中，首先测试第一个密钥，第一个密钥为一串 384 位的二进制比特序 列，改变其中 1bit 的数据，例如序列片段为“01100110001”，任意改变其中一位 则片段为“01000110001”。加密结果如图 3.7 所示。图上显示实验结果相差巨大。 然后测试第二个密钥，第二个密钥为人为给定，控制第一个密钥相同，只改变 第二个密钥，将密钥 1.253612458923145 改变成 1. 253612458923144，实验结果 如图 3.8 所示。尽管密钥只改变了 1e-15 后的小数位，但是结果也是截然不同。



(a) (b) (c)



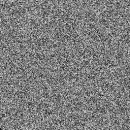
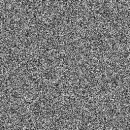
(d) (e) (f)

图 3.7 密钥 1 敏感性测试。(a)明文图像；(b)原始密钥加密后的图像；(c)改变密钥对原图加

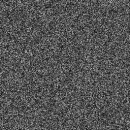
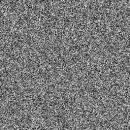
密的结果；(d)加密结果差异；(e)原始密钥对(b)的解密效果图；(f)改变密钥对(b)解密后的 图像。

27

中国知网 https:Www.cnki . net



(a) (b) (c)



(d) (e) (f)

图 3.8 密钥 2 敏感性测试。(a)明文图像；(b)原始密钥加密后的图像；(c)改变密钥对原图加

密的结果；(d)加密结果差异；(e)原始密钥对(b)的解密效果图；(f)改变密钥对(b)解密后的 图像。

3.5.2 直方图分析

加密图像的直方图分析是评估加密算法性能和安全性的常用工具之一，可 以帮助研究人员和工程师更好地理解和改进加密方案。通过比较明文图像和密 文图像的直方图分布， 能够直接地观察出加密算法对初始图像像素值分布的影 响程度。如果加密后的直方图与原直方图差异显著，且呈现出均匀或接近随机 分布的状态，通常说明该加密算法具有良好的扩散性和混淆性， 可以有效藏匿 原始图像的内容，加强系统安全。直方图能够显示图像的灰度级或颜色分量的 分布状况，进而体现图像的对比度特性。通过对比加密前后的对比度变化，可 以了解加密过程中是否导致了明显的视觉特征保留或损失。本实验分别对“鹦鹉” 和“蝴蝶”两幅图像的明文图像和加密后图像进行了直方图测试。结果如图 3.9 所 示。

28

中国知网 https:Www.cnki . net

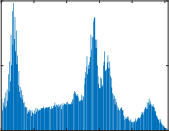
1000

**Frequency**  **Frequency**

500

1000

500

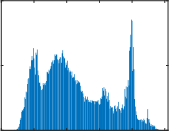


0

0 50 100 150 200 250

**Pixel grey value**

(a)



0

0 50 100 150 200 250

**Pixel grey value**

1000

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Frequency Frequency** | 500  1000  500 | 0   |  | | --- | |  |   0 50 100 150 200 250  **Pixel grey value**  (b)  0   |  | | --- | |  | |

0 50 100 150 200 250

**Pixel grey value**

(c) (d)

图 3.9 直方图测试。(a)(c)分别为鹦鹉和蝴蝶；(b)(d)为对应的密文图像直方图

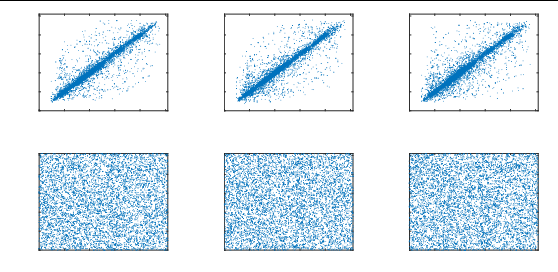
从图中可以看出，原始图像直方图分布不均匀，且存在一定规律。而通过加密 后，两幅图像的直方图都近乎平坦，呈现均匀分布。

3.5.3 图像像素相关性分析

在未加密的图像中，相邻像素通常存在一定的空间相关性，这是由于图像 的自然属性和成像过程决定的。良好的加密算法应能够显著降低甚至消除这种 相关性，使得攻击者无法通过观察密文图像中的像素间关系来推测出明文图像 的信息。相邻像素又分为三个方向，分别为水平方向、垂直方向和对角方向。 本节画出了“蝴蝶”图像的三个方向上加密前后的像素相关性，结果如图 3.10 所 示。从图中能够观察到原始图像三个方向上像素相关性都较高，而加密后的图 像像素分布较随机。文章中也通过数值分析了原始图像与密文图像的像素相关 性，结果如表 3.2 所示。表中的数据能够反映出原始图像三个方向上的像素相 关性都接近 1，而通过算法加密后像素相关性近乎为 0。因此通过此算法后图像 的相邻像素之间的相关性大幅度降低。

29

中国知网 https:Www.cnki . net

250

250

250

200

200

200

150

**Pixel value on location (x,y+1)**

**Pixel value on location (x,y+1)**

**Pixel value on location (x,y+1)**

150

150

100

100

100

50

50

50

0

0

0

0 50 100 150 200 250

0

50 100 150

**Pixel value on location (x,y)**

200

250

0 50 100 150 200 250

**Pixel value on location (x,y)**

**Pixel value on location (x,y)**

(c)

(a)

(b)

250

250

250

200

200

200

150

**Pixel value on location (x,y+1)**

**Pixel value on location (x,y+1)**

**Pixel value on location (x,y+1)**

150

150

100

100

100

50

50

50

0

0

0

0 50 100 150 200 250

50 100 150

**Pixel value on location (x,y)**

200

250

0

0 50 100 150 200 250

**Pixel value on location (x,y)**

**Pixel value on location (x,y)**

(d) (e) (f)

图 3.10 “蝴蝶”明文图像及密文图像的相邻像素分布。

在表 3.3 中对比了本方案与其他文献中算法对密文图像的像素相关性数值， 可以观察到本方案的像素相关系数更小，密文图像具有更高的安全性。

表 3.2 图像像素相关性系数

|  |  |  |  |
| --- | --- | --- | --- |
| 图像 | 水平方向 | 垂直方向 | 对角方向 |
| (256×256) | 明文图像 加密图像 | 明文图像 加密图像 | 明文图像 加密图像 |
| 蝴蝶 | 0.9309 0.0031 | 0.9269 -0.0072 | 0.8835 0.0013 |
| 鹦鹉 | 0.9563 0.0011 | 0.9406 0.0093 | 0.9148 -0.0014 |
| Lena | 0.9203 0.0008 | 0.9575 0.0024 | 0.9148 0.0006 |
| Cameraman | 0.9333 -0.0020 | 0.9565 0.0014 | 0.9130 0.0020 |

表 3.3 图像 Lena 加密后相关系数比较

图像 Lena (256×256) 论文方案 文献 [19] 文献 [49] 文献 [74]

像素相关系数

垂直方向 0.0024

-0.0090 0.0059 -0.0021

水平方向 0.0008

0.0015 0.0053 0.0083

对角方向 0.0006

-0.0120 0.0031 -0.0025

绝对值总和 0.0038

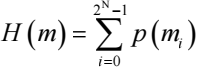
0.0225 0.0143 0.0129

3.5.4 图像熵分析

信息熵是衡量数据无序性或随机性的度量，对于图像来说，原始未加密的 图像通常具有较低的信息熵（对于灰度图像，理论上最大熵为 8 位灰度级对应 的熵值）。一个优良的图像加密算法应当能够让密文图像的熵尽可能接近最大熵。 因此，通过计算加密图像的熵并将其与理论最大熵对比，可以评估加密算法是

30

否成功地将原始图像的信息隐藏起来，提高了系统的安全性和保密性。高熵意 味着图像中像素值的分布更加均匀且随机，不易被攻击者使用统计特征进行分 析破解。通过对加密图像的熵进行分析，可以直观了解加密算法对图像信息扩 散程度的有效性。图像的信息熵定义为：

log2  (3.18)

其中，p(mi)是符号 mi 的概率，N 是每个符号 mi 对应的位数。表 3.4 列出了实验 的图像熵。从表中的数据能够得出，两副加密图像的熵都接近理想值 8。表 3.5 列出了与其他方案的比较。

表 3.4 图像信息熵

|  |  |  |
| --- | --- | --- |
| 测试图像 | 明文图像 | 密文图像 |
| 蝴蝶 | 7.4716 | 7.9970 |
| 鹦鹉 | 7.6569 | 7.9965 |
| Lena | 7.4429 | 7.9969 |
| Cameraman | 7.0097 | 7.9977 |

表 3.5 Lena 图像加密后信息熵比较

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 图像 Lena (256×256) | 论文方案 | 文献 [19] | 文献 [49] | 文献 [74] |
| 图像信息熵 | 7.9969 | 7.9939 | 7.9972 | 7.9971 |

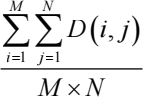
3.5.5 抗差分攻击测试

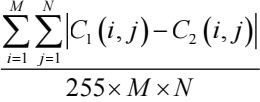
差分分析是一种针对密码系统的统计分析技术，攻击者通过观察输入和输 出之间的差异来推测密钥信息或其他秘密数据。在进行抗差分攻击测试时，通 常会模拟攻击者的行为，尝试构造一组具有特定差异的明文对，并计算它们经 过加密系统后输出密文之间的差异分布。如果这种差异能够保持随机且不可预 测，则表明该加密算法对差分攻击具有良好的抵抗力。

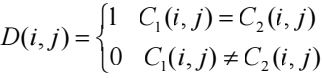
通常情况下，像素变化率 NPCR（Number of Pixels Change Rate）和标准化 平均变化强度 UACI（Unified Average Changing Intensity）是两个用来评估图像 加密质量的重要指标。NPCR 主要用于量化图像在加密前后像素值发生变化的 程度，而 UACI 则反映的是加密后图像像素值整体分布的变化情况，两者都被 规范化以提供一种统一且可比较的测量标准，它们被定义为：

31

中国知网 https:Www.cnki . net

*NPCR* = × 100% (3.19)

*UACI* = × 100% (3.20)

 (3.21)

其中，M 和 N 分别是图像的长和宽，C1 和 C2 是仅有一个像素差别的两个明文 图像进行加密后得到的密文图像。一般认为，NPCR 应大于 99.5893% ，UACI 的范围在[33.3703%,33.5541%]区间内，加密算法就能抵抗差分攻击[70]。

在本部分的实验中，首先对明文图像进行加密，然后改变其中一个像素值， 并再次进行加密，通过这两次加密得到的密文图像可以计算 NPCR 和 UACI 的 值。表 3.6 展示了实验结果。可以观察到算法在抵抗差分攻击方面具有良好的 性能。

表 3.6 加密图像 NPCR 和 UACI 值

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试图像 | NPCR | 通过/失败 | UACI | 通过/失败 |
| 蝴蝶 | 99.61% | 通过 | 33.48% | 通过 |
| 鹦鹉 | 99.59% | 通过 | 33.49% | 通过 |

3.5.6 抗噪声测试

抗噪声测试是一种评估图像加密算法在存在噪声干扰时的性能和安全性的 方法。在实际应用中， 图像在传输或存储过程中可能会受到多种干扰和噪声的 影响，这些因素可能会对加密图像的质量以及解密后图像的恢复效果产生不利 影响。密文图像添加不同程度的椒盐噪声后， 我们对其进行解密，目的是评估 加密系统的抗噪声能力以及解密后图像的可辨认性。如图 3.11 所示。从图表中 可以观察到，即使在加密图像中施加了不同程度的椒盐噪声干扰，相应的解密 后图像仍能维持足够的清晰度以实现有效的内容识别。

32

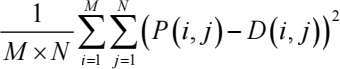
中国知网 https:Www.cnki . net



(a) (b) (c)

图 3.11 鹦鹉图像在添加不同椒盐噪声强度后的解密图像。从(a)到(c)，椒盐噪声强度分别为 0.10 、0.15、0.20。

为评估算法对抗噪声影响的性能，本文采用了峰值信噪比（Peak Signal to Noise Ratio，简称 PSNR）这一量化指标，用以衡量在同等噪声强度下系统的抗 干扰性能。换言之，PSNR 值越高，则代表系统对噪声的抵抗力越强。PSNR 的 定义为：

*MSE* =  (3.22)

*PSNR* = 10 lg  (3.23)

在这一过程中，P(i,j)与 D(i,j)分别代表尺寸为 M×N 的明文图像和加密后密文图 像在坐标(i,j)处对应的像素强度。表格 3.7 展示了在不同比例椒盐噪声影响下的 测试图像对应的 PSNR 值。通过分析该表格数据，我们能够确认该算法在面对 噪声攻击时展现出良好的抵抗能力。

表 3.7 不同噪声强度下的 PSNR 值

|  |  |  |  |
| --- | --- | --- | --- |
| PSNR（dB） | 椒盐噪声强度 | | |
| 0.1 | 0.15 | 0.2 |
| 蝴蝶 | 17.8264 | 16.1030 | 14.9190 |
| 鹦鹉 | 17.7775 | 16.1289 | 14.6736 |

3.5.7 抗裁剪测试

在数据传输过程中，有可能会出现信息缺失的情况，所以实验应该分析在 加密图像不完整的情况下是否能够通过算法进行破译。文中通过将部分加密图 像的像素值设为零，模拟了图像在裁剪后可能出现的效果。实验结果如图 3.12 所示。

33

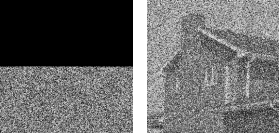
中国知网 https:Www.cnki . net



(a) (b)

(c) (d)

(e) (f)



(g) (h)

图 3.12 图像在不同程度裁剪下的解密图像。(a)-(g)为部分裁剪后的加密图像；(b)-(h)为与之 对应的解密图像。

从图中可以看出，解密图像会因为裁剪程度的增加而渐渐变得模糊，但是 图像中的内容仍能够辨认。并且表 3.8 中列出了解密图像的 PSNR 值，数据表 明该算法具有足够的鲁棒性。

表 3.8 不同裁剪程度下的 PSNR 值

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试图像 | 1/16 | PSNR 1/4(左上角) | 1/4(右下角) | 1/2 |
| 房屋 | 20.0277 | 14.2132 | 14.0193 | 11.5262 |
| 蝴蝶 | 19.9760 | 14.1076 | 13.9553 | 11.3391 |
| 鹦鹉 | 19.9018 | 13.8491 | 13.8394 | 10.9854 |

34

中国知网 https:Www.cnki . net

3.6 本章小结

本章节提出了一种融合了 Fisher-Yates 随机洗牌算法、DNA 编码技术和超混 沌 Lorenz 系统的综合图像加密方案。该方案首先依据待加密的原始图像生成一 个哈希值，该哈希值被进一步提炼转化为加密密钥，并且，将这一结果应用于 初始化超混沌 Lorenz 系统的核心参数设定。

在实施加密步骤时，方案采用了 Logistic-Tent 混沌映射与 Fisher-Yates 洗牌 算法的耦合策略，首先对明文图像进行深度的像素重排操作。 随后，采用具有 高级复杂性的超混沌 Lorenz 系统生成一系列混沌序列，这些序列扮演着动态掩 模的角色，贯穿并指导整个 DNA 编码过程的进行。最后，在完成了初步打乱 处理的图像区块基础上，采用基于 DNA 扩散原理的加密技术，逐块地对图像 信息进行深层次加密转换，最终形成高度安全的密文图像。

经过严格的实验测试与全面的安全评估分析表明，此方案在加密效率和安 全性方面展现出卓越性能，能有力抵御包括裁剪攻击在内的多种常见密码破解 手段，从而确保加密后的图像信息获得高强度的安全防护和保密性保障。

35

中国知网 https:Www.cnki . net

第四章 结合光混沌置乱、DNA 扩散和多目标粒子群优化算 法的图像加密方案

本章在第三章的基础上，引入了优化算法，并将混沌映射改为由激光器产 生混沌，以及对其中的 DNA 编码算法进行了一系列调整，具体来说本章研究 了一个将光学混沌、DNA 编码和 MOPSO 算法相融合的图像加密方案。在这一 方案中，主激光器（ML）驱动两对附属激光器产生两对同步的混沌信号，并使 激光混沌序列转换到 0-255 内以进行后续的加密操作。 加密阶段包括三个部分： 密钥生成、加扰和 DNA 编码扩散。在密钥生成阶段，使用 SHA-384 算法算出 输入图像的散列值，MOPSO 产生优化值。 在置乱阶段，使用上一阶段产生的 值进行异或运算，其值用于调制 ML 的偏置电流，从而驱动 TPSL 生成两对同 步混沌序列。使用混沌序列将图像的像素位置打乱后，再通过 DNA 编码规则 将图像像素进行扩散处理，接着在接收端使用两个相同的混沌序列对加密图像 进行解密和反向扩散。ML 、SL1 、SL2 为发送端，同时 SL3 、SL4 为接收端。

然后引入 MOPSO 算法。加密图像的所有参数被视为群体，每个粒子对应 一个密码图像。优化目标在于最大化密文图像的熵值，并同时降低密文图像中 相邻像素间的关联度。然后，选择 Pareto 主导粒子放入存储库中，循环获得最 佳粒子群位置，用于调制 ML 的偏置电流。在接收端部分，我们运用 SL3 和 SL4 激光器执行解密操作。通过与发送端激光器的同步处理，可以成功再现与 发送端完全一致的两组混沌序列。并使用它们来反向扩散和解密密码图像，即 可恢复原始图像。

4.1 加密系统模型

系统原理图如图 4.1 所示。ML 为主激光器，SL 为从激光器，BS 为分束器， CPFM 为共轭相位反馈镜，EOC 为电光转换器，PD 为光电探测器。

在该方案的光学混沌同步系统中， 具有注入锁定。该方案包括一个带有共 轭相位反馈镜（CPFM）的 ML 和两个具有相同 CPFM 的 SL ，CPFM 从 ML 反 射的共轭混沌被分束器（BS）分成两部分。一部分经过 BS1 反馈给 ML ，生成 混沌信号；另一部分注入 BS2 并分成四束，分别注入 SL1 、SL2 、SL3 和 SL4 。 为了实现两对激光器之间的高质量混沌同步，即 SL1 和 SL3 具有相同的内部参 数，SL2 和 SL4 具有相同的内部参数。 SL1 和 SL2 用于通过光电探测器（PD） 直接检测生成加密混沌序列，SL3 和 SL4 用于通过 PD 直接检测生成解密混沌

36

中国知网 https:Www.cnki . net

序列。通过系统的循环加密和粒子群优化， 即可得到密文图像。然后利用电光 转换器（EOC）将其变为光信号通过光纤链路进行传输，并在接收端通过 PD 将光信号转换为电信号。

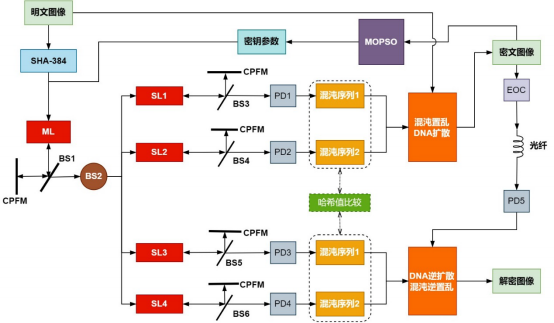
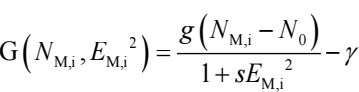


图 4.1 系统模型图

基于理论模型 Lang-Kobayashi（L-K）模型。本系统模型的具体方程如等式 (4.1)-(4.4)所示。

*E*M + *k*f*E*(4.1)  = 1+ i*a* ) *G* (*N*i, *E*i 2 )*E*i + *K*inj*E* (*t* −*τ*i )*e*−*iω*1*τ*i *ei*(*ω*2 −*ω*1 )*t* + *k*s*E*i\*(*t* −*τ*s )*e*−*iω*2*τ*s (4.2)



 (4.4)

其中下标 M 代表 ML ，i 代表四个从激光器的序列号。EM,i 代表 ML 和 SL 光 场的复振幅， NM,i 是激光器有源层中的载流子数密度 ， ‖*E*M ‖2 为光子数 ， *G*(*N*M, ‖*E*M ‖2 ) 代表增益函数。针对 ML 和 SL 器件，其内部参数设定包括以下 几点：α 代表着线宽增强系数，而 kf 和 τf分别对应 ML 器件接受相位共轭反馈

37

中国知网 https:Www.cnki . net

时的反馈强度和反馈时延；与此同时，kinj 和 τi 则是 SL 器件的注入强度和注入 时延参数。ks 和 τs 是来自 SL 的反射镜的反馈强度和总反馈时间延迟，G 是增益 函数。ML 和 SL 的直接偏置电流固定为*I*M,i = 2.2 × *I*th ，*Ith* 是激光器的阈值电流， *g* 是微分增益， *s* 是饱和系数， *N*0 是透明载流子数密度， *e* 是每个电子的电荷， *γ* 和*γe* 分别是光子衰减率和载流子衰减率， *ω* 是光的角频率。

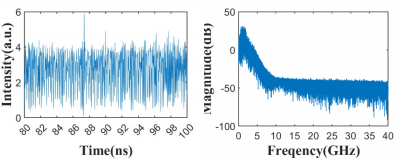
系统需要保持发射端 SL1 至 SL3 的同步，以及接收端 SL2 至 SL4 的同步。 为了保持同步，该方案中选择的系统的主要参数如表 4.1 所示。同时实验采用 四阶龙格-库塔方法来求解方程组(4.1)-(4.4)。

表 4.1 系统相关参数表

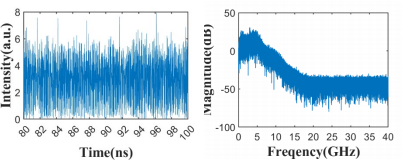
|  |  |  |
| --- | --- | --- |
| 参数符号 | 参数描述 | 参数值 |
| α | 线宽增长因子 | 3 |
| *τ*f | ML 反馈时延 | 1.2 ns |
| *kf* | ML 反馈强度 | 30 ns-1 |
| *IM,i* | 偏置电流 | 38.06 mA |
| *γ*e | 载流子衰减率 | 0.65 ns-1 |
| *γ* | 光子衰减率 | 496 ns-1 |
| *g* | 差分增益 | 1.2× 10-5 ns-1 |
| *N*0 | 透明载流子 | 1.25 × 108 |
| *s* | 饱和系数 | 5 × 10-7 |
| *kin*1,3 | SL1 ，SL3 的光注入强度 | 30 ns-1 |
| *kin*2,4 | SL2 ，SL4 的光注入强度 | 40 ns-1 |
| *ks* | SL1- SL4 的光反馈强度 | 50 ns-1 |
| *τ*1,3 | SL1 ，SL3 的光注入时延 | 3 ns |
| *τ*2,4 | SL2 ，SL4 的光注入时延 | 4 ns |
| *τs*1,3 | SL1 ，SL3 的光反馈时延 | 2 ns |
| *τs* 2,4 | SL2 ，SL4 的光反馈时延 | 5 ns |

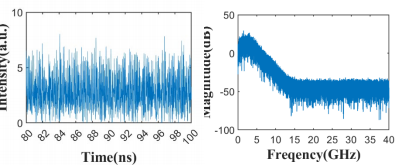
4.2 激光器动力学特性

ML 和 SL 所产生的信号在时间序列和功率谱方面的表现，在图 4.2 中予以 展示。从图中可以看出，三个时间序列都表现为类似噪声波动的随机强度脉冲， 并且每个激光器都具有较大的带宽。



(a) (b)





(c) (d)

(e) (f)

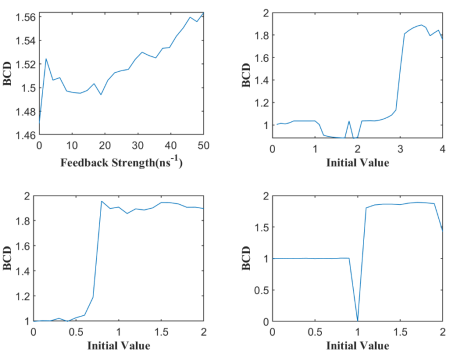
图 4.2 激光器混沌态的时间序列和功率谱。(a)-(b) ML; (c)-(d) SL1; (e)-(f) SL2.

方案中采用了分形维数这一量化手段，目的是为了衡量由激光输出产生的 混沌信号的内在复杂程度。混沌信号具有典型的自相似性以及复杂的多尺度结 构，而分形维数恰好能够有效捕捉并度量这类特性。通过计算混沌信号的分形 维数，可以对信号的非线性动力学性质以及其潜在的信息熵做出定量评估，这 对于理解和分析激光系统中的混沌行为至关重要。具体来说，论文利用盒维数 （BCD）这一手段来估算混沌系统的分维属性，从而深入理解其内在的复杂性。 实验中，本节记录了在不同反馈强度条件下激光混沌信号的 BCD 值，同时对具 有不同参数配置的 Logistic 映射、正弦映射和 Tent 映射也进行了 BCD 值的计算。 结果展示在图 4.3 中。从图中可以清晰看出，随着激光反馈强度的逐步降低，

相应的混沌序列的 BCD 值先经历了一个小幅下滑的过程，然后转而呈现上升态 势。值得注意的是，在整个反馈强度变化区间内，BCD 值都保持在一个相对较 高的水平，这有力地证明了论文的光学混沌系统即使在较低反馈强度下也能稳 定地处于高度复杂的混沌状态之中。

39

中国知网 https:Www.cnki . net



(a) (b)

(c) (d)

图 4.3 混沌序列的 BCD 值。(a)激光混沌信号；(b)Logistic 映射；(c)Sine 映射；(d)Tent 映射。

为了评估半导体激光器（SL）输出信号的复杂性，论文借助最大李亚普诺 夫指数（LLE）这一工具来判断系统是否进入了混沌状态； 当系统的最大 Lyapunov 指数(LLE)数值超过零时，即可确认该系统正处于混沌状态。在实验 中，注入强度 kinj 固定为 30 ns-1 ，然后探讨不同反馈强度对系统混沌特性的调控 作用。通过对激光器动态特性的计算，在本节中我们绘制了在该注入强度下 SL 输出的最大李亚普诺夫指数随反馈强度变化的曲线，参见图 4.4 (a)。从图中明 显看出，在保持注入强度不变的情况下，不论反馈强度如何调整，LLE 始终保 持大于零的状态，这验证了 SL 输出始终能够在各种反馈强度下维持混沌状态。

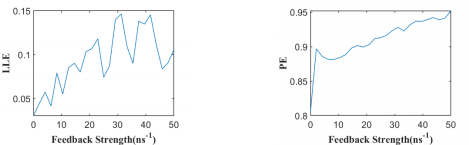
排列熵（Permutation Entropy, PE）作为一种非线性手段，用于评估时间序 列或信号的复杂程度，这一概念最初是由 Bandt 和 Pompe 两位研究者在 2002 年 的研究成果中首次引入并定义的。它通过分析时间序列数据中符号的相对顺序 来评估系统的动态特性[71] 。LZC（Lempel-Ziv Complexity）或称为 Lempel-Ziv Complexity Measure，是一种基于数据压缩理论的无参数复杂性度量方法。该方 法由 Abraham Lempel 和 Jacob Ziv 在 1976 年提出[72]，最初是作为衡量一个序列 自相似性和随机性的工具，后来也被应用于量化混沌信号以及一般时间序列的 复杂程度。在对序列进行分析时，若 LZC（Lempel-Ziv Complexity）值越高， 则说明该序列的复杂程度更大，也就是说，序列中包含的非重复模式元素更为 丰富。反之，如果 LZC 值较低，则说明序列具有更多的重复模式或更高的规律 性。在混沌动力学研究中，LZC 被用来评估混沌信号的内在结构复杂性，特别

40

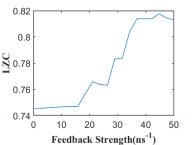
中国知网 https:Www.cnki . net

是在低维混沌系统的研究中，它能够提供一种有效的非线性动态特性描述手段。 随着混沌序列反馈强度、系统参数的变化，LZC 值的变化可以反映系统从简单 到混沌状态的转变过程及其内在的复杂性变化。

接下来，论文通过排列熵 (PE) 和 Lempel-Ziv complexity (LZC) 进一步量化 混沌信号的复杂程度。观察图 4.4（b）可以发现，在注入强度锁定为 30 ns-1 的 条件下，随着反馈强度的增强，PE 值呈现出稳步上升的趋势。而在图 4.4（c） 中，LZC 值同样表现出随着反馈强度增加而先增后稳的特点，这可能是由于当 反馈强度增大到一定程度时，系统进入了一个强烈的非线性运作区间，从而使 得混沌信号的复杂性逐步提高。



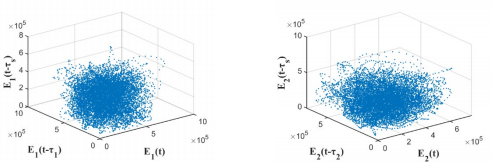
(a) (b)



(c)

图 4.4 SL1 的 LLE 、PE 和 LZC 值

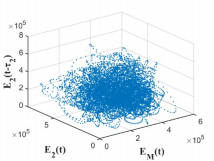
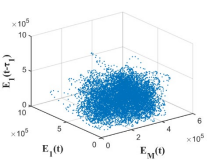
可以通过场 Ei 、Ei (*t* −*τ*i ) 、EM 吸引子来观察混沌的特征。从图 4.5 可以看 出，场吸引子随机分布，局部不稳定，全局稳定，表现出混沌的特征。这意味 着这些激光器在混沌态中。



(a) (b)

41

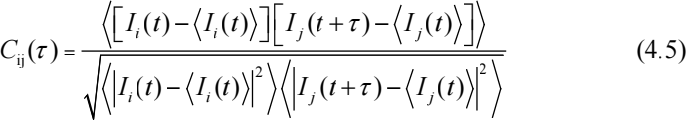
中国知网 https:Www.cnki . net



(c) (d)

图 4.5 SL 动力学特性的数值模拟。(a)-(b)分别是 SL1、SL2 的吸引子；(c)-(d)是 SL1 与 ML 、SL2 与 ML 之间的吸引子。

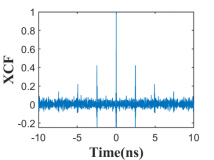
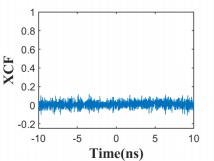
在本系统中，当且仅当 SL1 和 SL3 以及 SL2 和 SL4 处于同步状态时，才能 正确获取加密使用的混沌序列。一般来说，互相关效率（XCF）衡量的是系统 的同步质量，因此论文引入 XCF 为式 (4.5)。互相关（Cross-Correlation Function, XCF）是信号处理与统计学领域内的一个关键工具，它被用来评估两个随机变 量或信号在某种程度上的相似性或线性耦合程度。互相关函数计算的是一个信 号在另一个信号平移不同时间间隔（或空间位置）时的相似程度。



其中 Cij 为混沌强度的 XCF 值，⟨.⟩ 为时间平均值，τ 为时间延迟，i，j 代表对应 的两个激光器。图 4.6 分别显示了 SL1 和 SL3 、SL1 和 SL4 、SL2 和 SL4 、SL2 和 SL3 之间的相关系数。 实验发现，只有 SL1 和 SL3 、SL2 和 SL4 之间的 XCF 值为 1，而 SL1 和 SL4 之间或 SL2 和 SL3 之间的XCF 值大于或小于 1。这意味 着只有 SL1 到 SL3，以及 SL2 到 SL4 可以同步，否则不同步。

考虑到噪声，可能会导致发射端和接收端的激光器之间的偏置电流不匹配， 从而影响它们之间的同步。图 4.6 (e)中 SL1 和 SL3 之间 XCF 的仿真结果表明，

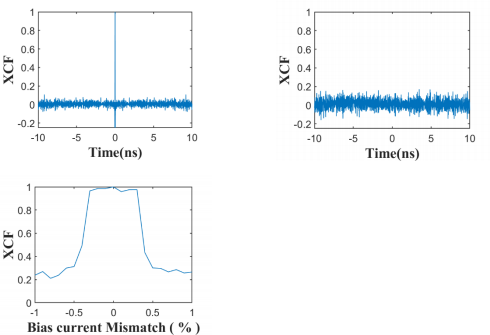
噪声引起的 0.3%的偏置电流失配对 XCF 的影响较小。



(a) (b)

42

中国知网 https:Www.cnki . net



(c) (d)

(e)

图 4.6 SL 的互相关系数图。(a) SL1 和 SL3; (b) SL1 和 SL4; (c) SL2 和 SL4; (d) SL2 和 SL3; (e) SL1 和 SL3 受到噪声影响后的 XCF 值。

4.3 图像加密算法

本方案的流程包括密钥生成、混沌置乱、DNA 编码/解码和粒子群优化过程。 具体的优化加密方案将在下面详细介绍。

4.3.1 密钥生成

首先，该研究通过应用 SHA-384 哈希算法对原始图像进行了处理，从而获 得了反映该图像特征的 96 位十六进制哈希值。接着，将这 96 个十六进制字符 转化成二进制形式，作为对输入图像进行后续处理的数据源。然后，这 384 比 特将被分成 8 比特一组，依次进行异或运算，将结果再次转换成十进制数。除 以 232 即可得到 0-1 范围内的十进制 r1。流程如图 4.7 所示。

其次，通过对自然环境噪声进行采样，获得由浮点数组成的噪声信号数组 N [73] 。并将 Ni 作为粒子群的初始粒子。在第一次迭代中，我们从集合 N 中检索 第一个值 r2。在后续迭代中，r2 通过 MOPSO 系统获得。 r1 和 r2 之间进行异或 运算后的值用于调制 ML 的偏置电流。

43

中国知网 https:Www.cnki . net

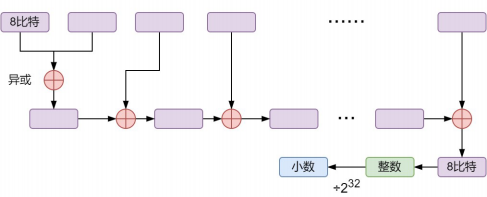


图 4.7 r1生成流程图

获得 r1 和 r2 后，ML 驱动两对从激光器（TPSLs）产生同步光学混沌信号。 从 SL1 和 SL2（或 SL3 和 SL4）输出的混沌时间序列中取出图像大小为 M×N 长度的混沌序列 si（i 代表激光器序列号），并将其值转换为方程式(4.6)中的运 算后，将序列映射到 0-255 之间。

*key*i = mod (floor (*r*1 × *s*i ) , 255), *i* = 1, 2 (4.6) 其中 floor()为向下取整运算，i 代表激光器序列号。经过公式转换后即得到密钥。

4.3.2 混沌置乱

在图像置乱阶段，本研究采用了一种混沌排序混排算法与 Zigzag 扫描排序 法相结合的方式，对图像像素进行了深度的混乱重排处理。步骤如下：

步骤 1：将图像像素矩阵转换为 M×N 长度的序列 I，每个像素位置对应于 密钥生成步骤中生成的 key1。

步骤 2 ：将密钥 key1 按升序排列后，与之对应地调整图像序列的位置，由 此得到重新排列后的图像序列 I'。

步骤 3：通过以下公式将 I'变换为矩阵，其中 M 和 N 分别是图像的行数和 列数，输出 Pc 是 M×N 大小的矩阵。

*Pc* = reshape (*I* ', *M* , *N*) (4.7)

步骤 4：对图像 Pc 的各个像素值进行 Z 形循环读取，如图 4.8 所示，然后将 得到的序列重构为图像 P。经过上述操作，得到置乱后的图像 P。

44

中国知网 https:Www.cnki . net

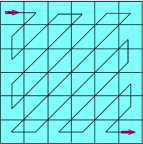


图 4.8 zigzag 扰乱像素。

4.3.3 DNA 加密

在 DNA 加密阶段，我们将对先前完成置乱处理的图像进行扩散加密操作。 具体步骤如下：

步骤 1：将块大小设置为 4×4。如果置乱矩阵 P 的行数或列数不满足 4 的整 数倍，用零填充以获得 P'，即 P 的行数和列数分别为 M'和 N'，然后将 P'分为块。

步骤 2：将 key2 转换为矩阵 R，如式(4.8)所示。

*R* = reshape (*key*2, *M* ′, *N*′ )

步骤 3 ：R 是 DNA 运算所需的矩阵，根据块大小将 R 分成块。 步骤 4：通过以下操作确定 DNA 扩散的方式：

*x*1,2 = mod (round (*r*2 × 104 ),8)+1 *x*3 = mod (round (*r*1 × 104 ), 4)

*x*4 = mod (round (*r*1 × 104 ),8)+1

(4.8)

(4.9) (4. 10) (4. 11)

其中 x1,2分别决定了置乱矩阵 P 和混沌矩阵 R 的 DNA 编码规则，其 1~8 的 整数值分别对应 DNA 规则中的 8 种编码方式；x3 决定了四种运算模式中的一种， 显然它的整数值范围是 0 到 3，其中 0 代表加法，1 代表减法，2 代表异或，3 代表 DNA 运算中的同或；x4 代表 DNA 解码方法，与编码方法类似。

步骤 5：将输入的置乱矩阵 P 和混沌矩阵 R 分为大小为 4×4 的{*p*1,*p*2,*p*3…}和 {*r*1,*r*2,*r*3…}子块，对每个小块进行编码生成 DNA 序列{*p*1', *p*2', *p*3' …}, {*r*1', *r*2', *r*3' …} 。 使用对应的块(*p*i',*r*i')进行 DNA 运算，得到{*q*1,*q*2,*q*3...} ，并编码为“A” ， “T” ，“G”和“C”，由 DNA 序列组成块。利用 x4 的整数值确定的 DNA 编码规则， 将由“A” 、“T” 、“G” 、“C”组成的每个子块转换为二进制值，然后将其转换为密 文图像对应的像素值。第一个块 *q*1 直接进行传输，第二个块 *q*2 在传输前与 *q*1

45

中国知网 https:Www.cnki . net

进行 DNA 运算。该操作块将继续与 *q*3 进行运算，后续块将按此方式依次进行 DNA 运算。流程如图 4.9 所示。

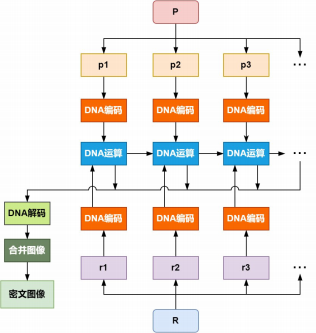


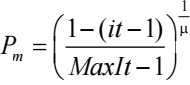
图 4.9 DNA 扩散流程

步骤 6：将每个 DNA 序列块按规定方式解码后组合起来生成密文图像。

4.3.4 多目标粒子群算法应用

在多目标粒子群优化算法中，论文引入了自适应网格存储库，为了决定是 否将某些解决方案添加到存档中，存储当前所有帕累托主导粒子以产生分布良 好的帕累托前沿，该前沿根据当前需要进入存储库的粒子位置生成网格空间， 在网格坐标系统中，粒子的位置以其各自的目标函数值来确定。

粒子群高效的收敛速度可能使其在多目标优化时收敛于局部最优解，因此 引入变异算子，它可以在搜索开始时影响所有粒子。另外值得注意的是，在不 断迭代的过程中，变异的发生会致使受到影响的粒子数目逐渐减少。变异发生 的概率遵循公式 (4.12)，其中 Pm 代表粒子的变异概率，it 代表当前迭代周期数， MaxIt 则表示总的迭代次数，而 μ（设定为 0.1）为预设的变异率常数。

 (4.12)

在该方案的具体配置中，我们设置了种群规模为 40 个个体，迭代次数上限 为 60 次。种群记忆库中可存储最近 20 个优秀粒子的信息。关于惯性权重参数，

46

中国知网 https:Www.cnki . net

起始值设定为 0.5，并随着每一次迭代以 0.99 的递减率进行调整。此外，个体 学习因子和群体学习因子分别被设定为 1.5 和 2，以调整个体和全体的学习能力。 同时，网格划分的精度被设定为 7，以细化搜索空间。群体位置边界设置为(0, 4]，粒子速度限制在[- 2, 2]，具体实施步骤如下：

步骤 1：利用环境噪声取样值或 SL1 的激光混沌序列初始化粒子群中的粒 子位置，用于调制 ML 的偏置电流。根据方程(4.13)，初始参数范围限制为(0, 4]。 从 *s*1中间取 40 个值，速度初始值均设置为 0。

*x*(*i*) = mod (*s*1i, 4) (4.13)

步骤 2 ：ML 驱动 SL 生成加密系统所需的混沌序列。此外，计算每个粒子 （对应的图像）的熵和相邻像素之间的相关性，并创建一个网格存储库来保存 帕累托主导粒子在存储库中以优化粒子的位置。

步骤 3：在存储库中筛选一个最佳值。根据网格确定的粒子位置，尽量不选 择多次出现的个体， 以增加多样性。根据方程式(4.14)-(4.15)，计算选择概率 p， 然后使用轮盘赌算法选择最优值。

*g* = exp (−2× *N*i )



(4.14)

(4.15)

其中 p 是选择概率，Ni 是存储库中每个粒子的出现次数。

步骤 4：根据式(2.19)-(2.20)计算下一代粒子的速度和位置。并将其放入约 束处理机制中。

步骤 5：在步骤 4 之后，我们将新一代粒子所确定的位置数值导入加密系统 内，进而以此对原始的明文图像实施加密处理，将其转化为密文形式。根据密 文图像，通过计算得到每个粒子对应的目标函数值。

步骤 6：应用变异算子。在实验中，当变异算子生成的新位置所对应的适应 度优于当前粒子所在位置的适应度时，会选择用变异算子的位置取代当前粒子 的位置进行更新；反之，若变异位置的适应度不优于当前位置，则粒子位置保 持不变，不予更新。

步骤 7：挑选出适应度最优的粒子并将它们插入到存储库中。

步骤 8：重复步骤 3~7，直到迭代结束。

步骤 9：在存储库中选出最优粒子作为加密系统的最佳值。该算法的伪代码 如图 4.10 所示。

最后，用这个挑选出来的值调制 ML 的偏置电流。

47

中国知网 https:Www.cnki . net

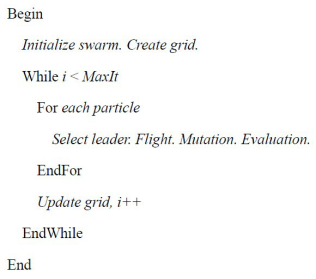


图 4.10 MOPSO 伪代码

4.3.5 解密流程

在通过光纤传输密文图像之前，为了确保原始真实图像能够被正确恢复，

需要在发送和接收两端利用哈希算法计算并比较两对混沌序列的摘要信息。同 时，在解密过程中，使用 SL3 和 SL4 进行解密操作。由于 SL1 和 SL2 产生的混 沌信号并未用于光纤链路中的传输，攻击者无法通过截取这两者的混沌序列来 获取 SL1 和 SL2 的参数，因此，攻击者无法实现与 SL1 和 SL2 混沌系统的同步， 从而无法解密这些信息。

具体来说， 图像的解密操作实质上是对加密步骤执行的反向操作。在通过 同步 SLs 系统得到密钥之后，通过对密文图像执行逆置乱和 DNA 扩散反运算， 即可还原出原始图像。加解密耗时不同，在加密过程中需要经过迭代优化选出 最佳的图像，耗时较长，解密只需要将所得的密文图像经过解密步骤即可还原。 具体耗时如下表所示， 由表中数据可得解密效率较高，耗时差距还与实验所用 机器性能有关。

表 4.2 所提出方案解密图像耗时

|  |  |  |  |
| --- | --- | --- | --- |
| 图像 | Baboon | Lena | Cameraman |
| 解密耗时 (s) | 0.3595 | 0.3341 | 0.3783 |

48

中国知网 https:Www.cnki . net

4.4 加密算法安全性分析

本节将通过算法对“Baboon” 、“Lena”和“Cameraman”三张图像进行加密，结 果如图 4.11 所示。从图形演示中可见，此算法不仅适用于灰度图像的加密与解 密处理，同样也能高效应对彩色图像的加密与解密任务。图 4.12 分别显示了三 张图的 MOPSO 结果。

如图 4.11 所示，经过加密处理后的原始图像已无法直接辨识，也无法从中 抽取有意义的信息，唯有采用正确的密钥进行解密，才能还原出原始图像。在 图 4.12 中，红点是存储库中的粒子，黑叉代表飞行的粒子，横坐标是 8 减去图 像的熵，纵坐标为密文图像的像素相关性。



(a) (b) (c)



(d)



(g)



(j)

(e)



(h)



(k)

(f)



(i)

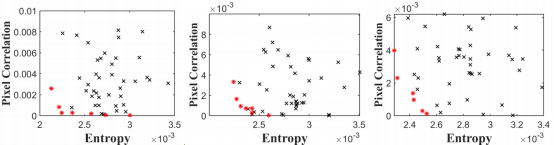


(l)

图 4.11 仿真结果。(a)-(j)原始图像；(b)-(k)密文图像；(c)-(l)解密图像

49

中国知网 https:Www.cnki . net



(a) (b) (c)

图 4.12 MOPSO 选择结果图。(a) Baboon； (b)Lena；(c)Cameraman。

同样我们对原图和解密后的图像做了均方误差分析，计算得到测试图像的 均方误差皆为 0 。说明该方案的加解密处理能够保证图像的完整性，不会对图 像精度有损失。

4.4.1 密钥空间以及密钥敏感性测试

在本系统中，加密密钥是从图像的哈希值计算出的。经过测试， r1 的有效 精度可 以达 到 10-16 ，r2 的有 效精度为 10-15 。 因此 ，总 的密钥空 间为 2384 ×1016 ×1015 ，明显大于 2100 。该研究表明，文中提出的算法对于暴力破解攻 击具有显著的有效抵抗力。

在加密与解密过程中，即便是密钥发生极其微小的改动，也可能导致对同 一 张图 像产 生截然 不同的 加密 效果及 解密结 果。 例如， 加密时 r1 为 0.3173238974768790 ， 解密时，只 要改变 其中任意 一 位，例 如 r1' 变为 0.3173238974768791，解密图像就会发生巨大变化。控制 r1 保持不变，修改 r2 的值。比如 r2 是 2.366548995447862，在解密的时候修改为 2.366548995447852， 情况还是一样。如图 4.13 和图 4.14 所示，虽然密钥稍有不同，但解密后的图像 完全不同。





(a) (b) (c) (d)

图 4.13 密钥敏感性测试。(a) 原始图像； (b) 用 r1 加密； (c) 用 r1 解密； (d) 用r1′ 解密。

50

中国知网 https:Www.cnki . net

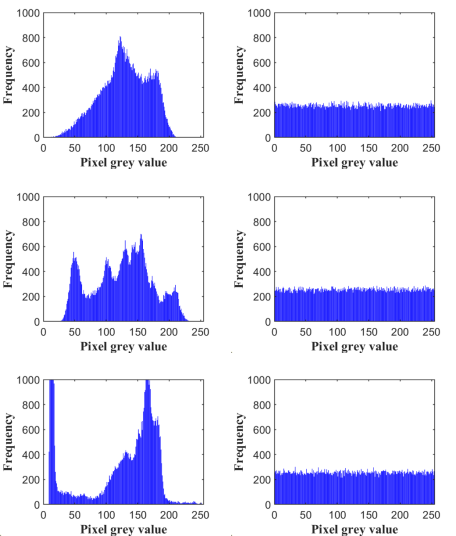


(a) (b) (c) (d)

图 4.14 密钥敏感性测试。 (a) 原始图像； (b) 使用 r2 加密； (c) 用 r2 解密； (d) 用 r2′ 解密。

4.4.2 直方图测试

明文图像及其对应的密文图像的灰度值分布状况如图 4.15 所示。通过观察 图像可知，原始图像的灰度分布并不均匀，而加密后的密文图像其灰度分布却 接近均匀状态。这一结果有力地证明了文中所提出的加密方法能够有效地防止 基于直方图分析类型的攻击行为。



(a) (b)

(c) (d)

(e) (f)

图 4.15 直方图测试。 (a)-(e)分别是 Baboon、Lena、Cameraman 的直方图； (b)-(f)分别是对

51

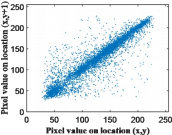
中国知网 https:Www.cnki . net

应的密码图像直方图。

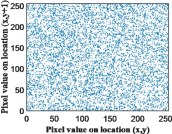
4.4.3 像素相关性测试

通常情况下，普通图像中相邻像素点在水平、垂直及对角线上存在着较强 的关联性。然而，对于加密后的密文图像，期望其相邻像素间的相关性大大降 低。为了验证加密前后像素关联性的变化，文章选取了若干对来自普通图像及 相应密文图像的相邻像素对（涵盖上述三种方向），并分别计算这些像素对的相 关系数。相关实验结果以图形形式进行了展示。

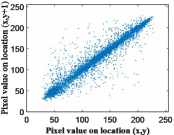
在本次试验中，“Lena”图像在横向、纵向及对角线方向上的相邻像素相关 性，及其对应的加密后密文图像中像素的相关性，已通过图 4.16 进行了详细展 示。此外，表 4.2 汇总了加密前后各类图像的相关系数对比数据，而表 4.3 则列 举了与其他研究文献中结果的对照情况，从对照数据来看，本论文提出的方案 比其他对比文献的像素相关性数值更小，说明该加密优化方案效果更好。从图 4.16 可以明显看出，原始图像中相邻像素点之间存在着强烈的关联性，这一点 也在表 4.2 中相邻像素相关系数较大的数值上得到了印证。并且密文图像的像 素值是随机地分布在 0-255 之间，相关系数小于 0.01 。这显示了加密图像中各 个相邻像素间的关联度极为微弱。



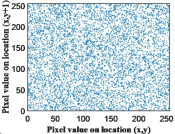
(a)



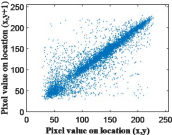
(d)



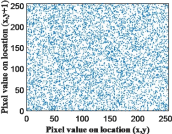
(b)



(e)



(c)



(f)

图 4.16 Lena 图像加密前后三个方向的相关系数。 (a)-(c) Lena 图像的水平、垂直和对角线 相关系数； (d)-(f)密文图像在水平方向、垂直方向以及对角线方向上计算得到的相关系数。

52

中国知网 https:Www.cnki . net

表 4.2 图像的像素相关性

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 图像 | 水平方向 | | 垂直方向 | | 对角方向 | |
| 明文 | 密文图像 | 明文 | 密文图像 | 明文 | 密文图像 |
| Baboon | 0.8672 | 0.00011 | 0.8366 | 0.0013 | 0.7857 | 0.00052 |
| Lena | 0.9303 | 0.00029 | 0.9575 | 0.00046 | 0.9148 | 0.00039 |
| Cameraman | 0.9333 | -0.000014 | 0.9596 | 0.000051 | 0.9130 | 0.00037 |

表 4.3 像素相关性对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Image(256×256) | Lena(ours) | 文献[70] | 文献[74] | 文献[52] |
| 水平方向 | 0.00029 | 0.0053 | 0.0083 | -0.0004 |
| 垂直方向 | 0.00046 | 0.0059 | -0.0021 | 0.0037 |
| 对角方向 | 0.00039 | 0.0031 | -0.0025 | -0.0378 |
| 数值总和 | 0.00114 | 0.0143 | 0.0129 | -0.0345 |

4.4.4 图像熵分析

在加密步骤中，由于原始图像处于有序状态，故其信息熵往往小于经过加 密处理后的图像信息熵。特别是针对拥有 256 级灰度值的灰度图像，理想的加 密结果应该是密文图像的信息熵尽可能接近 8。当密文图像的信息熵达到这一 理想阈值时，表明该图像加密算法具备有效抵抗熵攻击的能力。表 4.4 列出了 几幅图像的熵，以及与其他文献的比较结果。从表中观察得到，通过论文所提 出方案加密后的图像的信息熵要高于其他文献，所以本方案的加密效果更好， 并且每幅密文图像的熵接近理想值 8。

表 4.4 图像信息熵及比较

|  |  |  |  |
| --- | --- | --- | --- |
| 图像(256×256) | Baboon | Lena | Cameraman |
| 明文图像 | 7.2374 | 7.4429 | 7.0097 |
| 所提出方案 | 7.9977 | **7.9977** | **7.9976** |
| 文献[49] | - | 7.9972 | 7.9974 |
| 文献[74] | - | 7.9964 | 7.9964 |
| 文献[70] | - | 7.9971 | - |

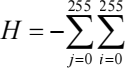
一维熵能够体现图像灰度值的集聚特性，但在揭示图像灰度值的空间排列 规律方面存在局限性。因此，为了充分描述图像的空间特性，我们需要在原有 的一维熵基础上引入能够捕捉灰度空间分布特性的新指标，进而构建出能够反 映图像二维空间信息的二维熵。为了刻画图像的空间特性，可以选择一种可行

53

中国知网 https:Www.cnki . net

的方法是利用相邻像素的平均灰度值作为衡量灰度分布空间属性的特征指标。 这种方法将像素的灰度值与邻域平均灰度值相结合，构建特征二元对(i,j)，其中 i 代表像素自身的灰度值（取值范围为 0 到 255 之间），j 表示相邻像素的平均灰 度值（0 <= j<= 255）。图像的二维熵可以定义为：

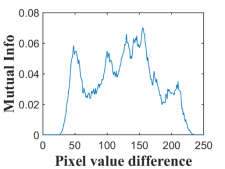
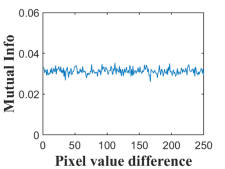
 (4.16)

*pij* log *pij* (4.17)

其中特征二元对(i,j)由 f(i,j)表示。在实验中，通过考虑图像尺寸比例为 M×N 的 情况下计算得到的二维图像熵如表格 4.5 所示。文中进一步展示了"Lena"原始图 像与其对应的加密图像间相邻像素的互信息关系，这一对比情况在图 4.17 中有 直观表现。原始未加密图像的邻近像素之间呈现出较强的关联性；然而，在经 过加密处理后的图像中，相邻像素的相关性显著下降。结合对一维及二维图像 熵的全面考察，我们可以得出结论：该论文提出的加密方案在提高安全性方面 展现出了良好的效果。

表 4.5 图像二维熵

|  |  |  |  |
| --- | --- | --- | --- |
| 图像 | Baboon | Lena | Cameraman |
| 明文图像 | 7.2347 | 7.4429 | 7.0097 |
| 密文图像 | 7.9903 | 7.9900 | 7.9899 |



(a) (b)

图 4.17 图像相邻像素之间的互信息。(a) Lena 原始图像；(b)加密的 Lena 图像。

4.4.5 抗差分攻击分析

本次测试中，改变 Baboon 明文图像不同位置的像素值，测试对应的 NPCR 和 UACI。结果如表 4.6 所示，并且将结果与其他文献中的值进行了对比，对比 结果如表 4.7 所示。NPCR 和 UACI 的期望值分别为 99.6094%和 33.4635%。根

54

中国知网 https:Www.cnki . net

据表格数据的分析表明，两个关键评估指标的平均数值与理论预期值极为吻合。 这有力地验证了文中提及的加密算法在抵抗基于差分分析的安全攻击上具备显 著的有效性。

表 4.6 Baboon 图像不同位置的 NPCR 和 UACI

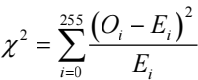
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 变换位置 | | | | | |
|  | (1,1) 96→95 | (23,45) 47→48 | (145,180) 177→ 176 | (204,221) 163→ 164 | Average |
| NPCR (%) | 99.615 | 99.635 | 99.577 | 99.603 | 99.6075 |
| UACI (%) | 33.439 | 33.404 | 33.423 | 33.534 | 33.45 |

表 4.7 NPCR 与 UACI 的比较

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 图像 Lena (256×256) | 本方案 | 文献[49] | 文献[74] | 文献[52] | 文献[65] |
| NPCR (Avg %) | 99.5936 | 99.6427 | 99.6207 | 99.61 | 99.228 |
| UACI (Avg %) | 33.4784 | 33.4741 | 33.4125 | 33.5 | 30.147 |

4.4.6 *χ*2 测试结果

卡方检验用于定量描述图像偏离完全均匀分布的程度。其计算公式如下：

 (4.18)

式中 i 为灰阶强度，Oi 为灰阶 i 的出现频率，Ei 为灰阶 i 的预期出现频率。当显 著性水平为 α=0.05 时，8 位灰度图像的临界值为 *χ*2 (255, 0.05) = 293.2478 ，得 到的密文图像值必须低于临界值，我们对一些图像进行了测试，结果如表 4.8 所示。可以看出得到的值都低于临界值，并且卡方值越小，图像灰度分布越均 匀，安全性越高。结果如表 4.8 所示。

表 4.8 卡方检验

|  |  |  |  |
| --- | --- | --- | --- |
| 图像 | Baboon | Lena | Cameraman |
| 明文图像 | 57852 | 39613 | 110720 |
| 所提出方案 | 260.5625 | 254.9401 | 277.3482 |
| 结论 | 通过 | 通过 | 通过 |

4.4.7 抗噪声和裁剪攻击

在这次实验中，我们对密文图像“Cameraman”分别施加了 10% 、15%以及

55

中国知网 https:Www.cnki . net

20%不同程度的椒盐噪声干扰，随后进行了解密处理。图 4.18 的结果表明，即 使加入噪声，图像内容仍然可以区分，表 4.9 给出了噪声攻击下原始图像与相 应解密图像之间的 PSNR。结果表明该方案对于抵抗椒盐噪声攻击有良好效果。



(a) (b) (c)



(d) (e) (f)

图 4.18 抗椒盐噪声攻击测试。 (a) 噪声强度 0.1 ； (b) 噪声强度 0.15 ； (c) 噪声强度 0.2；

(d)-(f) 对应于噪声强度的解密图像。

表 4.9 受到噪声影响后原始图像与解密图像之间的 PSNR

|  |  |  |  |
| --- | --- | --- | --- |
| 测试图像 | Baboon | Lena | Cameraman |
| 0.1 | 34.6188 | 34.5493 | 34.3758 |
| 0.15 | 33.0535 | 32.8597 | 32.7221 |
| 0.2 | 31.9000 | 31.7048 | 31.5364 |

在图像传输过程中，有可能会出现关键信息的损失。因此，研究中需要验 证受损图像能否成功恢复，为此，我们先将图像的部分像素设为 0 以模拟裁剪 效果，然后对缺失部分的密文图像进行解密处理。如图 4.19 所示，即使密文图 像在不同区域丢失了大量数据，解密后的图像依旧能够保持一定程度的可识别 性。表 4.10 展示了在裁剪前后，原始图像与解密图像间的 PSNR 值。这些结果 有力证明了该方案对于抵抗裁剪攻击具有较好的效果。

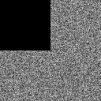
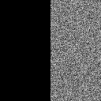
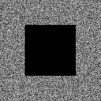
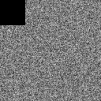
通过与其他文献的比较，发现该方案能够很好地满足安全性的要求。该方 案优点在于：DNA 编码和运算规则的选择是预先协商好的，此外，接收器只能 接收发射器处的 ML 信号，而不能接收发射器处的 SL 信号。因此，由于 SL 参 数的未知性，窃听者很难重建混沌动力学或实现混沌同步。这意味着安全性得 到进一步增强。

56

中国知网 https:Www.cnki . net

表 4.10 受到裁剪攻击后原始图象与解密图象之间的 PSNR

|  |  |  |  |
| --- | --- | --- | --- |
| 测试图像 | Baboon | Lena | Cameraman |
| 1/16 | 39.2291 | 39.1908 | 38.8488 |
| 1/4 | 33.4896 | 33.1977 | 33.0366 |
| 1/4 (in the middle) | 33.3140 | 33.1290 | 32.9681 |
| 1/2 | 30.4436 | 30.2574 | 30.0469 |



(a) (b) (c) (d)



(e) (f) (g) (h)

图 4.19 抗裁剪攻击测试结果。 (a) 1/16 裁剪； (b) 密码图像左上角的 1/4 裁剪； (c) 在密码 图像中间进行 1/4 裁剪； (d) 1/2 裁剪； (e)-(h)对应的解密图像。

4.5 本章小结

本章提出了一种综合运用多目标粒子群优化（MOPSO）、DNA 编码及光学 混沌原理实现的图像加密方法。首先分析了用于图像加密与解密过程中的光学 混沌结构，其中，通过主激光器（ML）驱动的从激光器（TPSL）产生两对同 步的混沌信号，并将这些信号映射到 0 至 255 的灰度范围以便于后续加密操作。 加密过程分为三个关键步骤：密钥生成、像素位置混淆以及基于 DNA 规则的 扩散处理。

在密钥生成阶段，采用初始图像的哈希值与经过 MOPSO 算法优化得到的 参数值进行异或运算，以此来动态调制 ML 的偏置电流，从而产生两对匹配的 混沌序列。这两对序列结合了初始图像的哈希信息，进而生成用于加密的两个 独立密钥。发送端利用这两个密钥分别对图像像素的位置进行随机置乱，并应 用预先定义的 DNA 编码规则对像素值进行扩散加密；接收端则利用共享的相 同密钥执行相应的解密和反向扩散过程以恢复原始图像。

在 MOPSO 框架内，优化参数被视为粒子群的位置属性，每个粒子对应一 个潜在的加密后图像。适应度函数采用矢量形式，考虑了密码图像的熵值和相

57

中国知网 https:Www.cnki . net

邻像素间的相关性。每一轮迭代后，帕累托最优解被存储于主导粒子库中，循 环更新最佳粒子群位置。

在光纤传输加密图像之前，为了验证混沌序列的一致性，通过两端执行相 同的哈希算法计算并比较两对同步混沌序列的摘要信息，确保接收端能够正确 还原实际图像。

实验结果显示，该加密方法表现出优秀的加密效果和安全性，能够有效抵 御多种针对图像的攻击手段。此外，该方案的安全性体现在两个方面： 一是 DNA 编码的选择和运算规则是预先协商且私有的；二是接收方仅能接收到发射 方经 ML 调控产生的混沌信号，而无法获取直接控制 SL 信号的能力，使得窃听 者难以复制混沌动力学或实现与发射端 SL 的同步，从而提高了密钥重建的难 度。这一特性加强了图像加密系统的安全性。

本章节将混沌映射这种描述混沌现象的数学模型改为由激光系统产生的真 正的物理随机信号，使得产生的混沌序列具有更好的不可预测性和不可复现性， 安全等级更高，并且激光混沌信号具有宽频谱特性，适用范围更广。引入的多 目标粒子群优化算法让加密过后的图像具有更好的性能表现。在图像 DNA 编 码运算阶段也较第三章进行了细微调整，图像的加密复杂度随之变高。

58

中国知网 https:Www.cnki . net

第五章 总结与展望

5.1 总结

在当前这个大数据时代背景下，数据安全的重要性日益凸显，它不仅关乎 到国家的安全战略与核心利益，也直接影响着每一个公民的个人隐私和权益保 护。随着数据量的爆炸性增长和信息交换的频繁程度加剧，确保数据在存储、 传输过程中的安全性成为了全球范围内的焦点议题。因此，在当今时代，信息 保密通信技术的研发与实践运用变得至关重要，特别是在保护数字图像信息安 全这一领域更是不可或缺，其研究成果对于防止敏感图像信息的非法获取和滥 用起到了决定性作用。

数字图像加密是一种将原始可视且易于理解的明文图像通过特定算法转化 为不可直接识别且难以复原有效内容的密文形式的过程。这一过程中，研究者 们积极探索并开发出各种高级加密技术以提高加密强度和抵抗破解的能力。混 沌理论作为自然界的奇妙现象之一，因其内在固有的伪随机性特质， 对初始条 件和系统参数具有极高的敏感依赖性，以及动态行为的高度复杂性等特点，让 基于混沌系统的加密方法研究逐渐成为保密通信领域的重要研究方向。利用混 沌理论设计的加密算法能够生成类似真随机数序列的密钥流，为数字图像提供 安全保障，大大增加了潜在攻击者还原原始图像的难度。此外，在科技不断进 步的驱动下，光电转换技术尤其是半导体激光器领域的创新，进一步拓宽了混 沌加密的应用前景。光混沌由于其独特的物理属性和高度不可预测性，在图像 加密领域展现出了巨大的潜力。部分研究者正致力于探索如何借助基于半导体 激光器产生的光混沌信号来实现高安全级别的图像加密技术，这更是为图像保 密通信开辟了全新的道路。

本文系统地介绍了混沌系统、光混沌系统、图像加密的基本理论，并结合 国内外相关文献，提出了两种基于混沌的图像加密方案。其一是基于 Lorenz 超 混沌和循环 DNA 编码的图像加密方案，该方案将 LTM 混沌、Lorenz 混沌与图 像加密结合，在置乱和扩散阶段达到良好的扰乱效果，加密图像能抵抗多种攻 击方式。其二是一种结合光混沌置乱、DNA 扩散和多目标粒子群优化算法的图 像加密方案，该方案将光混沌与图像加密相结合，并使用粒子群算法寻出最佳 的加密图像。

论文在第一章引言中主要介绍了此研究的背景与研究的意义， 阐述了激光 器动力学行为的发展历程和混沌图像加密的研究现状。

59

中国知网 https:Www.cnki . net

第二章集中探讨了混沌图像加密的理论基石及相关技术手段。该章首先详 尽解释了混沌的基本含义及其界定，并深入剖析了混沌的特性以及判断混沌状 态的手段。随后，论述了如何通过半导体激光器实现混沌信号的产生，重点讲 解了借助光注入、光反馈及光电反馈等技术手段，并且给出了相关动力学模型 及对应的数学方程式。接下来，该章节详细叙述了混沌图像加密的整体流程， 并讨论了在图像置乱和扩散阶段所采用的加密方法，其中包括经典的 Fisher- Yates 洗牌算法以及新颖的 DNA 编码技术。最后，本章还涵盖了粒子群优化算 法的基础知识，并具体列举了执行粒子群算法时的各个步骤，以展示其在图像 加密领域的应用潜力。

基于前两章所奠定的理论基础和研究成果，本文在第三章中创新性地提出 了一个集成了 Fisher-Yates 随机排列算法、DNA 编码方法以及超混沌 Lorenz 系 统的综合性图像加密方案。此方案首先依据待加密的原始图像生成一个哈希值， 该哈希值被进一步提炼转化为加密密钥，并将这些参数作为启动超混沌 Lorenz 系统运行的核心初始设定。 然后在加密阶段采用了 Logistic-Tent 混沌映射与 Fisher-Yates 洗牌算法的耦合策略，对明文图像进行深度的像素重排操作，并利 用具有高度复杂性的超混沌 Lorenz 系统生成一系列混沌序列。最后，在完成了 初步打乱处理的图像区块基础上，采用基于 DNA 扩散原理的加密技术，逐块 地对图像信息进行深层次加密转换，最终形成高度安全的密文图像。

在论文第四章中，提出了一种结合光学混沌、DNA 编码序列和 MOPSO 算 法的图像加密方案。首先，利用主激光器驱动四个副激光器产生同步混沌信号， 并将信号量化至 0-255 范围作为加密的基础。首先采用 SHA-384 算出输入图像 的散列值，再由 MOPSO 算法生成一组优化参数作为密钥。其次用优化参数异 或处理后调制激光器偏置电流，产生混沌序列以随机打乱图像像素的位置。最 后进一步对置乱后的像素应用 DNA 编码规则进行扩散加密。加密过后，运用 MOPSO 算法优化密文图像的熵和像素相关性，选取最优解调整混沌序列生成， 确保加密效果。接收端同样使用两对同步混沌序列，通过与发送端相同的混沌 信号同步，进行反向操作（即解密和逆向扩散），最终恢复原始图像。

综上，所提出的两种加密方案经过一系列的实验和安全性测试后，都能达 到预期的加密效果。但是在应用阶段，两种方法各有优劣。第一种方案使用的 是混沌映射这种数学仿真模型，便于我们进行理论分析和计算机仿真，算法计 算速度快、资源需求低，适合在各种计算平台上实现。它的劣势在于在计算机 上存储的数值会以有限精度进行计算，数据误差可能会导致混沌特性的退化， 并且它的伪随机性在极高安全需求的场合可能不如真随机的安全性高。

第二种方案使用的半导体激光器产生的混沌信号来进行加密。由于激光混 60

中国知网 https:Www.cnki . net

沌产生的是真正的物理随机信号，这种硬件级别的随机性具有更好的不可预测 性和不可复现性，适用于对安全性要求极高的场合。并且激光混沌信号具有较 宽的频谱，可以覆盖更宽的频率范围，而且可以与现有的光通信、光信息处理 系统无缝集成。它的劣势在于，系统复杂程度较高，需要精密的光学器件、稳 定的激光源和复杂的反馈控制系统；为了在一定范围内稳定地维持混沌状态， 需要精细的参数调节和实时监控，对操作和维护有一定要求，并且在大量产生 混沌信号时，会增加能源损耗。

5.2 展望

本论文中的基于混沌的图像加密系统，仍存在一些不足之处，还能够在后 续研究中进行优化。

（1）光混沌的优化

在加密系统内部，激光器生成的光混沌信号在互相关图谱中蕴含了时延特 征，这给攻击者提供了可能的机会，使其能够在相空间中重现系统的动力学行 为。鉴于此，研究者可以采用隐匿时延特征的混沌激光系统方案，强化系统的 安全性。

（2）加密算法的优化

在粒子群优化算法中，由于粒子调控的是主激光器的偏置电流，粒子的飞 行过程以及光混沌序列计算过程都需要迭代从而花费较长的时间，后续可以通 过降低算法复杂度来提高执行速度。

61

中国知网 https:Www.cnki . net

参考文献

[1] Ye G. A block image encryption algorithm based on wave transmission and chaotic systems[J]. Nonlinear Dynamics, 2014, 75(3):417-427.

[2] Pareek NK, Patidar V, Sud KK. Image encryption using chaotic logistic map [J]. Image and Vision Computing, 2006, 24(9): 926–934.

[3] Li C Q, Xie T, Liu Q, et al. Cryptanalyzing image encryption using chaotic logistic map [J]. Nonlinear Dynamics, 2014, 78(2): 1545-1551.

[4] N AP, J N F, M C. Encryption and decryption of images with chaotic map lattices. [J]. Chaos (Woodbury, N.Y.), 2006, 16(3):033118.

[5] 颜森林,迟泽英, 陈文建.激光混沌同步及其在光纤保密通信中的应用[J]. 中国 科学 E 辑:信息科学, 2004, (04):467-480.

[6] Li N, B Kim, D Choi, V N Chizhevsky, et al. Fast random bit generation with a single chaotic laser subjected to optical feedback [C]. Proceeding of SPIE, 2014, 9134: 913427.

[7] Haken H. Analogy between higher instabilities in fluids and lasers[J]. Physics Letters A, 1975, 53(1): 77-78.

[8] Ikeda K. Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system[J]. Optics Communications, 1979, 30(2): 257-261.

[9] 王云才. 混沌激光的产生与应用[J].激光与光电子学进展, 2009, 46(04):13-21.

[10] Lang R, Kobayashi K. External optical feedback effects on semiconductor injection laser properties[J]. IEEE Journal of Quantum Electronics, 1980, 16(3): 347- 355.

[11] Yiwen T, Qiliang L, Wenlong D, et al. Optical chaotic communication using correlation demodulation between two synchronized chaos lasers[J]. Optics Communications, 2021, 498.

[12] Rontani D, Locquet A, Sciamanna M, et al. Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback[J]. Optics letters, 2007, 32(20): 2960-2962.

[13] Li S S, Liu Q, Chan C S. Distributed Feedbacks for Time-Delay Signature Suppression of Chaos Generated From a Semiconductor Laser[J]. IEEE Photonics Journal, 2012, 4(5):1930-1935.

[14] D R, E M, D W, et al. Enhanced complexity of optical chaos in a laser diode with

63

中国知网 https:Www.cnki . net

phase-conjugate feedback. [J]. Optics letters, 2016, 41(20):4637-4640.

[15] Nianqiang L, Wei P, A L, et al. Time-delay concealment and complexity enhancement of an external-cavity laser through optical injection. [J]. Optics letters, 2015, 40(19):4416-9.

[16] A. B, P. R, E. K C, et al. Feedback Phase in Optically Generated Chaos: A Secret Key for Cryptographic Applications[J]. IEEE Journal of Quantum Electronics: A Publication of the IEEE Quantum Electronics and Applications Society, 2008, 44(2):119-124.

[17] Hu H, Su W, Liu L, et al. Electro-optic intensity chaotic system with varying parameters[J]. Physics Letters A, 2014, 378(3):184-190.

[18] Meitong Y, Hongxiang W, Yuefeng J, et al. Ultra-wideband chaotic optical communication based on electro-optic differential feedback loop[J]. Optics Communications, 2023, 545.

[19] Xingyuan W, Maochang Z. An image encryption algorithm based on hyperchaotic system and DNA coding[J]. Optics and Laser Technology, 2021, 143.

[20] Mi L, Xinyu Z, Yifeng H, et al. Confidentiality-enhanced chaotic optical communication system with variable RF amplifier gain. [J]. Optics express, 2019, 27(18):25953-25963.

[21] Wen H, Lin Y, Kang S, et al. Secure image encryption algorithm using chaos- based block permutation and weighted bit planes chain diffusion[J]. Iscience, 2024, 27(1).

[22] Liu X, Tong X, Wang Z, et al. A new n-dimensional conservative chaos based on Generalized Hamiltonian System and its’ applications in image encryption[J]. Chaos, Solitons & Fractals, 2022, 154: 111693.

[23] Liu Y, Jiang Z, Xu X, et al. Optical image encryption algorithm based on hyper- chaos and public-key cryptography[J]. Optics & Laser Technology, 2020, 127: 106171.

[24] Chandra K R, Raj B P, Prasannakumar G. An efficient image encryption using chaos theory[C]//2019 International Conference on Intelligent Computing and Control Systems (ICCS). IEEE, 2019: 1506-1510.

[25] QIU W, Jun YAN S. An image encryption algorithm based on the combination of low-dimensional chaos and high-dimensional chaos[C]//2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE). IEEE, 2019: 684-687.

64

中国知网 https:Www.cnki . net

[26] Jinwei Y, Wei X, Zhenyu Z, et al. Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation[J]. Chaos, Solitons and Fractals: the interdisciplinary journal of Nonlinear Science, and Nonequilibrium and Complex Phenomena, 2022, 162.

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

[28] Jithin K, Sankar S. Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set[J]. Journal of Information Security and Applications, 2020, 50102428-102428.

[29] Almasoud A S, Alabduallah B, Alqahtani H, et al. Chaotic image encryption algorithm with improved bonobo optimizer and DNA coding for enhanced security[J]. Heliyon, 2024.

[30] Roy M, Chakraborty S, Mali K, et al. Biomedical image security using matrix manipulation and DNA encryption[C]//Proceedings of International Ethical Hacking Conference 2019: eHaCON 2019, Kolkata, India. Springer Singapore, 2020: 49-60.

[31] Bencherqui A, Tahiri M A, Karmouni H, et al. Optimal algorithm for color medical encryption and compression images based on DNA coding and a hyperchaotic system in the moments[J]. Engineering Science and Technology, an International Journal, 2024, 50: 101612.

[32] N. H A, S. AA. SE-Enc: A Secure and Efficient Encoding Scheme Using Elliptic Curve Cryptography[J]. IEEE Access, 2019, 7175865-175878.

[33] Ismail R A. Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography[J]. IEEE Access, 2020, 83875-3890.

[34] Sajjad A, Afzal M, Iqbal W, et al. Kleptographic Attack on Elliptic Curve Based Cryptographic Protocols[J]. IEEE Access, 2020, PP (99):1-1.

[35] Ibrahim S, Alharbi A. Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography[J]. IEEE Access, 2020, 8: 194289- 194302.

[36] Silva-Garcia V M, Flores-Carapia R, González-Ramírez M D, et al. Cryptosystem Based on the Elliptic Curve With a High Degree of Resistance to Damage on the Encrypted Images[J]. IEEE Access, 2020, 8: 218777-218792.

[37] 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, 738507- 38522.

65

中国知网 https:Www.cnki . net

[38] Bo Z, Di X, Yong X. Robust Coding of Encrypted Images via 2D Compressed Sensing[J]. IEEE TRANSACTIONS ON MULTIMEDIA, 2021, 232656-2671.

[39] Chen G, Li D, Zhang J. Iterative gradient projection algorithm for two- dimensional compressive sensing sparse image reconstruction[J]. Signal Processing, 2014, 10415-26.

[40] Ghaffari A. Image compression-encryption method based on two-dimensional sparse recovery and chaotic system[J]. Scientific Reports, 2021, 11(1): 369.

[41] Shufeng H, Donghua J, Qianxue W, et al. High-quality visually secure image cryptosystem using improved Chebyshev map and 2D compressive sensing model[J]. Chaos, Solitons and Fractals: the interdisciplinary journal of Nonlinear Science, and Nonequilibrium and Complex Phenomena, 2022, 163.

[42] Xiao J, Ying X, Yiyuan X, et al. Exploiting optical chaos for double images encryption with compressive sensing and double random phase encoding[J]. Optics Communications,2021,484126683-.

[43] Wang X, Su Y. Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform[J]. Scientific Reports, 2020, 10(1): 18556.

[44] Wei H, Donghua J, Yisheng A, et al. A Novel Double-Image Encryption Algorithm Based on Rossler Hyperchaotic System and Compressive Sensing[J]. IEEE ACCESS, 2021, 941704-41716.

[45] Xingyuan W, Yining S. Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform. [J]. Scientific reports, 2020, 10(1):18556-18556.

[46] Xie Y, Li J, Kong Z, et al. Exploiting Optics Chaos for Image Encryption-Then- Transmission[J]. Journal of Lightwave Technology, 2016, 34(22):5101-5109.

[47] Li L, Xie Y, Liu B, et al. Optical image encryption and transmission with semiconductor lasers[J]. Optics and Laser Technology, 2019, 119105616-105616.

[48] Wenlong D, Qiliang L, Yiwen T, et al. A robust and multi chaotic DNA image encryption with pixel-value pseudorandom substitution scheme[J]. Optics Communications, 2021, 499.

[49] Qin L, Congxu Z. A new one-dimensional chaotic map for image encryption scheme based on random DNA coding[J]. Optics and Laser Technology, 2023, 160.

[50] Wang X, Li Y. Chaotic image encryption algorithm based on hybrid multi- objective particle swarm optimization and DNA sequence[J]. Optics and Lasers in

66

中国知网 https:Www.cnki . net

Engineering, 2021, 137106393-.

[51] Kun Z, Dong W, Jinhui S, et al. Cross-utilizing hyperchaotic and DNA sequences for image encryption[J]. Journal of Electronic Imaging, 2017, 26(1):013021-013021.

[52] Zefreh Z E. An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions[J]. Multimedia Tools and Applications: An International Journal, 2020, 79(33-34):24993-25022.

[53] Xiaolin W, Bin Z, Yutong H, et al. A novel colour image encryption scheme using rectangular transform-enhanced chaotic tent maps[J]. IEEE Access, 2017, 1-1.

[54] Xue H, Du J, Li S, et al. Region of interest encryption for color images based on a hyperchaotic system with three positive Lyapunov exponets[J]. Optics and Laser Technology, 2018, 106506-516.

[55] Wang A, Wang Y, He H. Enhancing the Bandwidth of the Optical Chaotic Signal Generated by a Semiconductor Laser With Optical Feedback[J]. IEEE Photonics Technology Letters, 2008, 20(19):1633-1635.

[56] Li T Y, Yorke JA. Period three implies chaos[M]. Springer, 2004.

[57] Young L S. Dimension, entropy and Lyapunov exponents[J]. Ergodic Theory and Dynamical Systems, 1982, 2(1): 109-124.

[58] Langley L N, Shore K A. Effect of phase-conjugate optical feedback on the intensity noise in laser diodes. [J]. Optics Letters, 1993, 18(17): 1432-1434.

[59] Sattar Z A, Shore K A. Phase Conjugate Feedback Effects in Nano-Lasers[J]. IEEE Journal of Quantum Electronics, 2016, 52(4):1100108.

[60] Liao Y H, Lin F Y. Dynamical characteristics and their applications of semiconductor lasers subject to both optical injection and optical feedback[J]. Optics Express 2013, 21(20): 23568-23578.

[61] Wu Y, Wang Y C, Pu L, et al. Can fixed time delay signature be concealed in chaotic semiconductor laser with optical feedback? [J]. IEEE Journal of Quantum Electronics, 2012, 48(11): 1371-1379.

[62] Lorenz E. Deterministic nonperiodic flows[J]. Journal of the Atmospheric Sciences, 1963, 20: 267-285.

[63] Pujari S K, Bhattacharjee G, Bhoi S. A hybridized model for image encryption through genetic algorithm and DNA sequence. Procedia Computer Science, 2018, 125: 165-171.

[64] Sreelaja N K, Pai G A V. Stream cipher for binary image encryption using ant colony optimization based key generation. Applied Soft Computing, 2012, 12(9):

67

中国知网 https:Www.cnki . net

2879-2895.

[65] Ahmad M, Alam M Z, Umayya Z, et al. An image encryption approach using particle swarm optimization and chaotic map. International Journal of Information Technology, 2018, 10(3): 247-255.

[66] Liu B, Wang L, Jin Y H, et al. Improved particle swarm optimization combined with chaos. Chaos, Solitons & Fractals, 2005, 25(5): 1261-1271.

[67] J. Kennedy and R. Eberhart. Particle swarm optimization[J]. Proceedings of ICNN'95 - International Conference on Neural Networks, Perth, 1995, pp. 1942-1948.

[68] P. N, A. Z and A. E. Pareto Multi Objective Optimization. Proceedings of the 13th International Conference on. 2005, pp. 84-91.

[69] ALVAREZ G, LI S. SOME BASIC CRYPTOGRAPHIC REQUIREMENTS FOR CHAOS-BASED CRYPTOSYSTEMS[J]. International Journal of Bifurcation

and Chaos, 2006, 16(8):2129-2151.

[70] Wenlong D, Qiliang L, Yiwen T. Image encryption-then-transmission combining random sub-block scrambling and loop DNA algorithm in an optical chaotic system[J]. Chaos, Solitons and Fractals: the interdisciplinary journal of Nonlinear Science, and Nonequilibrium and Complex Phenomena, 2021, 153(P1).

[71] C. B, B. P. Permutation entropy: A natural complexity measure for time series - art. no. 174102[J]. Physical review letters, 2002, 88(17):4102.

[72] Lempel A, Ziv J. On the complexity of finite sequences[J]. IEEE Transactions on information theory, 1976, 22(1): 75-81.

[73] Liu H, Kadir A, Sun X. Chaos-based fast colour image encryption scheme with true random number keys from environmental noise[J]. IET Image Processing, 2017,

11(5):324-332.

[74] Xingyuan W, Shengnan C, Yingqian Z. A chaotic image encryption algorithm based on random dynamic mixing[J]. Optics and Laser Technology, 2021, 138.

68

中国知网 https:Www.cnki . net