分类号

UDC

密级

编号



**全日制专业硕士学位文**

**基于混沌的图像加密技术研究**

**学位申请人：** **张辉**

**专** **业** **领** **域** **：** **控制工程**

**校** **内** **导** **师** **：** **赖强** **副教授**

**答辩日期：**2023 年 5 月 26 日

中国知网 https:iiwww.cnki . net

**基于混沌的图像加密技术研究**

**摘要**

随着互联网与数字技术的飞速发展，各行业领域通过网络进行信息交互的行为日益 频繁。作为最常见的网络信息载体之一，数字图像不仅可以高效储存大量信息，还能很 好地展现出信息所蕴含的感情色彩。然而，数字图像在传输的过程中一旦被他人获取， 其蕴含的可视化信息极易面临泄露的风险。因此，图像信息安全的保护工作尤为重要， 而图像加密技术作为一种保护图像信息安全的有效方法备受关注。混沌系统作为一种非 线性系统具备众多优良的特性，如遍历性、初始条件敏感性以及不可预测性等。 根据以 上特性，研究人员将混沌系统与图像加密技术进行了有机结合，混沌图像加密技术应运 而生。

为了更好地保护图像的信息安全，本文利用混沌系统生成的混沌序列设计了三种混 沌图像加密算法，具体内容如下：

（1）提出了一种基于无平衡点混沌系统的混沌魔方变换图像加密算法（CMCT-IEA）。 首先，通过一种预处理操作方式将明文图像中的所有像素转换为一个三维魔方像素矩阵 并根据明文图像的尺寸大小生成相应的密钥。其次，利用密钥使本文所提出的无平衡点 混沌系统生成混沌序列，并根据预处理结果将混沌序列转换为与三维魔方像素矩阵大小 相同的三维魔方混沌矩阵。然后，利用三维魔方混沌矩阵对三维魔方像素矩阵进行置乱 与扩散操作。最后，经过三轮的置乱、扩散,得到密文图像。不同于以往的一些基于低维 空间的图像加密算法，CMCT-IEA 的所有加密操作过程都在三维空间中进行，这使得加 密结果具备更高的复杂度与随机性。

（2）提出了一种基于 2D-Price 混沌映射的索引同步置乱-扩散图像加密算法（ISPD- IEA）。首先， 对经典的 Price 函数进行改进，得到了一个新的二维 Price 映射，并将该映 射产生混沌序列转换为混沌矩阵。然后， 将混沌矩阵中的值进行放大、取整后再与初始 图像的像素进行加和取模运算得到随机像素矩阵。最后， 利用混沌矩阵对随机像素矩阵 进行两轮置乱-扩散操作，得到加密图像。ISPD-IEA 中的同步置乱-扩散机制能够在改变 图像的像素点位置的同时将图像的细微变化影响至所有像素点，具备较高的安全性与加 密效率。

（3）提出了一种基于忆阻超混沌正弦映射的比特级双循环移位图像加密算法 （MHSM-IEA）。首先，利用一个新的二维忆阻超混沌正弦映射生成混沌序列并转换为

与明文图像尺寸相同的混沌矩阵。其次， 混沌矩阵所有序列值经放大、取整操作后再与 明文图像进行加和、取模运算， 得到新的像素矩阵。然后，利用混沌矩阵对像素矩阵进

I

中国知网 https:iiwww.cnki . net

行位置索引置乱操作。然后，对置乱后得到的像素矩阵进行列/行方向上的比特级双循 环位移扩散，再将每一列/行的像素值与前一列/行的像素值进行异或运算。最终， 经过 两轮的置乱、扩散操作后得到密文图像。MHSM-IEA 结合了像素级别的位置置乱与比特 级别的双循环位移扩散，丰富了加密过程的多样性，有效保障了图像的信息安全。

实验仿真与安全性分析结果表明，本文所设计的三种图像加密算法都能够有效地保 护图像的信息安全，具备较高的实用性和安全性。

**关键词**：混沌系统，图像加密，置乱，扩散，安全性能分析

II

中国知网 https:iiwww.cnki . net

**THE RESEARCH ON IMAGE ENCRYPTION TECHNOLOGY BASED ON CHAOS**

**ABSTRACT**

With the rapid development of the Internet and digital technology, the interaction of information on the Internet has become more and more frequent in various fields. As one of the most common carriers of information on the Internet, digital images can not only store a large amount of information efficiently but also shows the emotional content of the information well. The visual data it contains, however, is easily exposed to the risk of leakage if the digital image is captured by others during the transmission process. As a result, it is crucial to safeguard the security of image information, and image encryption technology has received a lot of attention as a successful method of doing so. Due to its nonlinear nature, chaotic system has many excellent characteristics, such as ergodic, initial condition sensitivity and unpredictability. For the above characteristics, researchers combine chaotic system with image encryption technology to obtain chaotic image encryption algorithm.

To explore more digital image encryption strategies, this paper makes use of chaotic sequences generated by chaotic systems and proposes three chaotic image encryption algorithms, the details are as follows:

(1) A chaotic magic cube transforms image encryption algorithm (CMCT-IEA) based on no-equilibrium chaotic system is proposed. Firstly, a new no-equilibrium chaotic system is used to generate chaotic sequences. Secondly, based on the size of the plain image, a pre-processing operation mode is utilized to transform the pixels in the plain image into a three-dimensional magic cube pixel matrix and generate the appropriate key. Then, the three-dimensional chaotic matrix is used to diffuse and scramble the three-dimensional pixel matrix. Finally, the cipher image is obtained after three rounds of permutation-diffusion operation. Different from some previous image encryption algorithms based on low dimensional space, all the encryption operations of CMCT-IEA are carried out in three-dimensional space, which makes the encryption results more complex and random.

(2) An index-based simultaneous permutation-diffusion image encryption algorithm (ISPD-IEA) based on 2D-Price chaotic map is proposed. First, the classical Price function is improved to obtain a new two-dimensional Price map, and the chaotic sequence generated by the map is transformed into a chaotic matrix. Then, the values of the chaotic matrix are enlarged, rounded, and then added and modulo with the pixels of the plain image to get a random pixel matrix. The simultaneous permutation-diffusion mechanism of ISPD-IEA has the ability to move pixels around in an image and simultaneously effect all pixels' minor modifications, which has high security and encryption efficiency.

(3) A bit-based double-loop shift image encryption algorithm based on memristor

III

中国知网 https:iiwww.cnki . net

hyperchaos sine map (MHSM-IEA) is proposed. Firstly, a new two-dimensional memristor sine map is used to generate chaotic sequences and convert them into chaotic matrices with the same size as the plain image. After amplification and integer operation, the sequence values of the chaotic matrix are added and modulo operation with the plain image to obtain a new pixel matrix. Secondly, chaotic matrix is used to scramble the pixel matrix. Then, the pixel matrix obtained after permutation is diffused by bit-based double-loop displacement in the direction of column/row, and the pixel values of each column/row are XOR computed with the pixel values of the previous column/row. Finally, the cipher-image is obtained after two rounds of permutation-diffusion operation. MHSM-IEA combines pixel-level positions scrambling for bit-level double-cycle displacement diffusion to enrich the diversity of the encryption process and effectively ensure the information security of the image.

Experimental simulation and security analysis results show that the three image encryption algorithms designed in this paper can effectively protect the information security of the image, with high practicability and security.

**Key Words :** chaotic system, image encryption, permutation, diffusion, security performance analysis

IV

中国知网 https:iiwww.cnki . net

目 录

[第一章 绪论 1](#bookmark1)

[1.1 课题的研究背景与意义 1](#bookmark2)

[1.2 混沌图像加密国内外研究现状 2](#bookmark3)

[1.3 本文的主要研究内容 5](#bookmark4)

[第二章 混沌理论与图像加密基础 7](#bookmark5)

[2.1 混沌理论 7](#bookmark6)

[2.1.1 混沌的定义及特点 7](#bookmark7)

[2.1.2 混沌系统的判定标准 8](#bookmark8)

[2.1.3 几种常见的混沌系统 9](#bookmark9)

[2.2 密码学基础知识 11](#bookmark10)

[2.2.1 密码编码学 12](#bookmark11)

[2.2.2 密码分析学 12](#bookmark12)

[2.3 混沌图像加密基础 13](#bookmark13)

[2.3.1 混沌理论与密码学的联系 13](#bookmark14)

[2.3.2 混沌图像加密技术 13](#bookmark15)

[2.3.3 混沌图像加密算法的设计 16](#bookmark16)

[2.4 本章小结 17](#bookmark17)

[第三章 基于无平衡点混沌系统的混沌魔方变换图像加密算法 18](#bookmark18)

[3.1 无平衡点混沌系统的设计与分析 18](#bookmark19)

[3.2 图像加密算法介绍 21](#bookmark20)

[3.2.1 算法的加密过程 21](#bookmark21)

[3.2.2 算法的解密过程 25](#bookmark22)

[3.3 算法仿真分析 25](#bookmark23)

[3.3.1 仿真结果 25](#bookmark24)

[3.3.2 效率分析 26](#bookmark25)

[3.4 算法的安全性能分析 27](#bookmark26)

[3.4.1 统计特性分析 27](#bookmark27)

[3.4.2 密钥安全分析 30](#bookmark28)

[3.4.3 差分攻击分析 31](#bookmark29)

[3.4.4 鲁棒性分析 32](#bookmark30)

[3.5 本章小结 33](#bookmark31)

[第四章 基于 2D-Price 混沌映射的同步置乱-扩散图像加密算法 34](#bookmark32)

[4.1 2D-Price 混沌映射的设计与分析 34](#bookmark33)

[4.2 ISPD 图像加密算法 36](#bookmark34)

中国知网 https:iiwww.cnki . net

[4.3 算法仿真分析 40](#bookmark35)

[4.3.1 仿真结果 40](#bookmark36)

[4.3.2 效率分析 40](#bookmark37)

[4.4 算法的安全性能分析 41](#bookmark38)

[4.5 本章小结 46](#bookmark39)

[第五章 基于忆阻超混沌正弦映射的图像加密算法 47](#bookmark40)

[5.1 二维忆阻耦合超混沌映射的设计与分析 47](#bookmark41)

[5.2 图像加密算法介绍 50](#bookmark42)

[5.2.1 算法的加密过程 50](#bookmark43)

[5.2.2 算法的解密过程 54](#bookmark44)

[5.3 实验仿真与性能分析 54](#bookmark45)

[5.3.1 仿真结果 54](#bookmark46)

[5.3.2 性能分析 55](#bookmark47)

[5.4 本章小结 62](#bookmark48)

[第六章 总结与展望 64](#bookmark49)

[6.1 研究工作总结 64](#bookmark50)

[6.2 未来工作展望 65](#bookmark51)

[参考文献 66](#bookmark52)

中国知网 https:iiwww.cnki . net

**第一章** **绪论**

**1.1** **课题的研究背景与意义**

随着互联网与多媒体技术的蓬勃发展，网络逐渐成为了主流的信息交互平台，大多 数人都将信息以文字、图像、音频以及视频等形式进行网络传输[1]。相较于其它信息媒 介，数字图像兼具直观表达信息的特点以及高效的信息存储性能，因此被广泛应用于各 个领域。然而，互联网是一个开放且有迹可循的信息交互平台，图像在利用其进行储存 或传输的过程中很容易被窃取，这可能导致图像中的可视化信息遭受泄露。特别是对于 一些包含“敏感”信息的图像，如一些军事图像、医学图像、商业图像及个人隐私图像 等，这些图像的信息一旦被他人获取，可能造成难以估量的损失。因此， 如何有效保护 数字图像的信息安全变得尤为重要[2][3][4] 。图像加密作为一种极其可靠的图像保护技术 之一，能够将具备可视化信息的图像变为毫无特征的噪声图像，并且只有在密钥完全正 确的情况下才能得到初始图像[5][6][7]。

在图像加密技术发展的初期，研究人员根据文本信息加密原理设计出了一种简单的 数字图像加密方案。根据数字信息的储存特点将数字图像视作一组二进制数据流，再利 用一些数据加密方法对该数据流加密，进而实现图像加密。然而， 图像中的各像素一般 需要用 8 位或更多位的二进制数表示，这使得图像所有的像素经转换后数据量十分庞大， 使用传统的文本信息加密方式对其加密时效率较低[8][9]。另外，图像的特殊信息存储方 式使得其内部一些区域中的像素之间具有很强的相关性，因此图像转换成后得到的二进 制数据流具有很高的冗余度，使用传统的文本信息加密方式可能无法有效保护图像得信 息安全。为克服上述问题，研究人员根据图像的本质特点提出了一些针对性更强的图像 加密方案，主要有光学加密与数字信号加密两种方案[10]。其中，光学加密方案一般是在 图像的采集至成像过程中直接进行加密，而数字信号加密方案主要是在图像的储存与传 输过程对图像进行加密操作。由于光学图像加密方案需要在采集至成像的过程中进行加 密，只能依靠特殊的硬件设备才能实现图像加密，因此数字信号加密方案的应用范围更 加广泛。数字信号加密方案主要是通过改变图像像素的排列方式与数值大小，使得图像 变成无法获取任何信息的噪声图像，进而保障图像信息的安全。随着信息安全的需求不 断提高，研究人员在设计图像加密算法时结合了不同的技术理论，所使用的技术理论包 括混沌理论[11][12][13]、量子理论[14][15]、压缩感知技术[16][17]、DNA 编码技术[18][19]以及一些 数学模型[20][21]等。其中，混沌理论因其具备众多优良特性而成为图像加密领域应用最广 泛的理论技术之一。

混沌作为一种具备非线性动力学行为的类随机现象广泛且客观地存在于现实世界， 其最显著的特征表现为系统初始状态的变化决定着系统的动态演变趋势与结果。通过分

1

中国知网 https:iiwww.cnki . net

析可知，混沌系统所具备的非周期性、初始状态敏感性、不可预测性等独特性质分别与 图像加密中密文无序性、密钥敏感性、明文敏感性等要求十分契合[22] 。因此，基于混沌 系统的图像加密算法研究早已成为信息安全领域内的研究热点之一。目前，大多数混沌 图像加密算法都具备一种较为固定的设计模式[23]。首先对密钥进行计算进而得到混沌系 统的初值参数，随后混沌系统经迭代多次后可生成加密所需的混沌序列，最后利用混沌 序列设计出相应的加密机制[24][25]。近年来，随着计算机与密码分析技术的不断提升，许 多较为简易的混沌图像加密算法无法有效保障图像的信息安全。因此，改进现有的一些 混沌加密算法或提出新的混沌加密算法等工作迫在眉睫。

**1.2** **混沌图像加密国内外研究现状**

1963 年，美国学者 Lorenz 在气象预测的研究中首次发现“蝴蝶效应 ”，并提出了著 名的 Lorenz 系统，自此掀起了混沌领域的研究热潮[26] 。1989 年，Matthews 首次将混沌 理论与密码学进行结合，设计了一种新型的信息加密方案[27]。该方案利用一个改进的 Logistic 混沌映射生成的混沌序列，并将混沌序列作为一种流式序列密钥。1998 年， Fridrich 设计了一个基于二维 Baker 映射的图像加密方案[28]。该方案通过二维 Baker 映 射得到混沌序列，再利用混沌序列来打乱图像像素点的位置，最终将初始图像变为无法 辨认的噪点图。这是混沌图像加密的首次亮相， 也为图像加密策略提供了一种全新的设 计思路。此后，研究人员根据该设计思路提出了一种常规的混沌图像加密方案[29][30][31] ， 其结构如图 1-1 所示。

|  |
| --- |
| 密钥 |

|  |
| --- |
| **混沌系统** |

|  |
| --- |
| 混沌序列 |

|  |  |
| --- | --- |
|  |  |

|  |
| --- |
| 明文图像 |

|  |
| --- |
| **置乱** |

|  |
| --- |
| **扩散** |

|  |
| --- |
| 密文图像 |

加密机制

图 1-1 常见的混沌图像加密方案结构图

Fig. 1-1 The structure of common chaotic image encryption scheme

由图 1-1 可知，常见的混沌图像加密方案的加密过程为：首先，混沌系统在种子密 钥的作用下生成了相应的混沌序列；然后，利用混沌序列设计出新的加密机制，即“置

2

中国知网 https:iiwww.cnki . net

乱”与“扩撒”；最后，明文图像经加密机制作用下转变为密文图像。随着研究的不断深 入，人们对混沌图像加密算法的研究重心由加密算法的可行性逐渐转变为加密算法的安 全性及加密效率。因此，各类衡量混沌图像加密算法安全性能指标相继被提出[32][33][34] 。 由图 1-1 可知，混沌图像加密方案的关键“节点”在于混沌系统以及加密机制部分。因 此，提升混沌系统的性能与构建有效的加密机制是设计、改进混沌图像加密算法最重要 的两个途径。

（1）混沌系统的研究现状

低维混沌系统因具备结构简单、系统复杂度低等特点而被广泛应用于图像加密算法 中[35][36]。随着信息安全技术的发展， 基于一些简单的低维混沌系统所设计的混沌加密算 法无法保证图像信息的安全，因此国内外研究人员尝试通过提高混沌系统的混沌特性来 提升混沌图像加密算法的安全性能。Behnia 等人通过在 Tent 映射中引入一个新的控制 参数提升了混沌映射的混沌区间及混沌特性，并基于该混沌系统设计了一个性能优异的 混沌图像加密算法[37] 。Zhou 等人将 Logistic 映射、Tent 映射以及 Sine 映射中的任意两 个映射进行耦合，最终获得了 3 个不同的调制混沌系统，仿真测试结果表明所得的调制 混沌系统均具备更优异的非线性动力学特性，利用它们设计的混沌图像加密算法具有更 好的加密效果[38] 。Liu 等人针对 Logistic 映射密钥空间小、混沌序列选取困难等不足，

通过引入变分技术得到了一个新的动态参数 Logistic 映射，该混沌映射能够根据可变化 的变分参数得到动态变化的混沌序列，最终设计出的混沌加密算法具备较高的加密性能 [39]。除了对低维的混沌系统进行改进之外，也有学者采用高维混沌系统甚至超混沌系统 设计图像加密算法。Wang 等人将 Chen 混沌系统与 Sine-logistic 映射进行耦合调制，最 终得到了一个新的四维混沌系统，并利用该混沌系统设计了一种新的彩色图像加密算法。 实验结果表明，该算法能够有效地抵御多种攻击[40]。Lone 等人基于三维混沌映射与 DNA 编码技术设计了一种高安全性的图像加密算法，该算法根据 DNA 运算规则与异或运算 使得三维 Arnold 映射生成的密钥序列，再利用三维 Logistic 混沌映射得到的 3 个密钥生 成序列对图像进行置乱与扩散操作[41] 。Liu 等人提出了一种具有 4 个正 Lyapunov 指数 的超混沌四维分数阶离散 Hopfield 神经网络系统(4D-FDHNN)，并在此基础上设计了一 种分形模型置乱方法以及 Hilbert 动态随机扩散方法，仿真结果和安全分析实验表明了 该算法具有良好的效率和较高的安全性能[42]。

（2）混沌图像加密机制研究现状

加密机制的优劣在很大程度上决定着混沌图像加密算法的加密性能，尤其是安全性 与加密效率。混沌图像加密算法的加密机制大多采用了“置乱-扩散”的加密模式，其改 进思路一般可通过设计出更可靠的“置乱 ”与“扩散 ”机制，进而提升混沌图像加密算 法的安全性能与加密效率。当前，加密机制的主流实现形式包括像素级和比特级。基于 像素级的图像加密算法是将图像像素作为算法的最小加密单元，在加密图像时往往能够 具备较好的安全性与效率，因此能够适用于大多数加密场合。而基于比特级的图像加密

3

中国知网 https:iiwww.cnki . net

算法是将图像像素的比特位作为最小操作单位，在加密图像时能够在更为微观的层面上 改变图像信息，适用于对加密安全性要求较高的应用场合，但加密所耗费的时间成本较 高。

对于像素级图像加密，通常将明文图像视为一个像素矩阵，再对矩阵中的各像素单 元实施加密操作。Cheng 等人将 Tent 映射生成的混沌序列与 S 盒加密原理进行结合，设 计了一种高效率的图像加密算法，通过循环移位以及查表的方式直接对图像像素进行加 密操作，有效地减少了加密算法中的运算量，进而提升了加密效率[43] 。Zhou 等人提出 了一种基于超混沌与压缩感知技术的图像加密算法，该算法利用一种三维超混沌系统生 成的混沌序列对压缩后的明文图像像素矩阵进行加密，因此，其加密过程拥有较高的加 密效率[44]。Hua 等人提出了一种基于二维 Logistic-Sine 耦合映射的图像加密算法，该算 法基于像素层面设计了一种二维平面置乱方法与流式扩散算法，能够以较快的速度实现 像素的位置置乱与像素的数值变化[45]。Anwar 等人基于混沌理论提出了一种基于像素排 列的加密技术，并且该技术能够将加密后得到的密文图像伪装成普通图像，从而避开攻 击者的注意[46] 。Xian 等人提出了一种基于螺旋变换混沌分块置乱（CSBS）与混沌数字 选择扩散（CDSD）混沌图像加密算法。该算法首先基于混沌系统设计了一种新的像素 扫描置乱方法，有效地降低了算法的时间和空间复杂度。其次， 在扩散过程中使用了两 组混沌序列对像素矩阵进行选择性的扩散操作。实验表明， 该算法在具备较高加密效率 的同时还能有效抵御各类攻击[47] 。Kumar 等人基于增强型索普变换与 Zig-zag 扫描卷积 （ETS-ZSC）提出了一种独特的图像加密算法。该算法通过对初始图像像素和超混沌系 统生成的混沌序列进行匹配进而得到 Logistic 映射的初始值，再利用 Logistic 映射对平 面图像进行洗牌操作和生成用于卷积操作的临界网格[48] 。Hussain 等人提出一种多向置 乱-扩散混沌图像加密算法，首先利用一个四维混沌系统产生混沌序列，再通过扩展操作 沿像素平面的两个对角方向同时进行置乱与扩散操作，最后利用混沌序列完成像素值的 替换与变化。该算法经一系列评估测试证明其具备较高的效率及安全性[49]。

对于比特级图像加密，通常是将明文图像的各像素转换成长度为 8 位的二进制串进 而得到对应的二进制矩阵，再对该二进制矩阵进行“置乱”与“扩散”操作，最终完成 对初始图像的加密工作[50] 。Zhu 等人首次提出了一种基于比特级变换的图像加密算法， 该算法采用 Arnold 映射进行位级排列并且利用Logistic 映射进行扩散，该算法表明在进 行位级排列时能够同时改变图像像素的位置与值[51] 。Xu 等人提出了一种基于比特级的 分段线性混沌映射图像加密算法。该算法首先将图像信息转变为两组等长的二进制序列， 随后再利用一种新的扩散策略使两组序列进行相互扩散，最后在混沌映射的控制下完成 两组序列间二进制元素的交换工作[52] 。Wang 等人基于比特级置乱与 DNA 编码技术设 计了一种超混沌图像加密算法，该算法首先分别将图像像素与一个六维超混沌系统生成 的混沌序列转换成二进制序列，再对所得的二进制序列进行 DNA 编码操作，最后根据 编码规则对编码后的序列进行计算，完成图像加密[53] 。Basha 等人利用混沌映射、循环

4

中国知网 https:iiwww.cnki . net

位移和异或操作设计了一种位级混沌彩色图像加密技术。该技术首先将彩色图像分解为 红、绿、蓝分量矩阵后并分别将他们转换为二进制矩阵， 然后利用循环位移和异或操作 对各二进制矩阵进行扩散操作，最后再利用混沌映射对各二进制矩阵内的元素进行交换 操作。该方案能够在单轮加密的情况下表现出较好的加密效果[54]。

不论是对原有的混沌图像加密算法进行改进还是设计一个新的混沌图像加密算法， 其研究的关键在于混沌系统的选取以及加密机制的设计。选取合适的混沌系统更容易生 成加密所需的混沌序列，进而提升图像加密算法的抵抗攻击能力。一个出色的加密机制 不仅能提高算法的安全性，还能提升算法的加密效率。

**1.3** **本文的主要研究内容**

本文研究了混沌图像加密技术的设计与改进工作，尝试探究混沌系统的性能提升与 不同加密机制对加密算法效率及安全性能的影响，进而设计出了一些独具特点的混沌图 像加密算法。主要研究内容如下：

第 1 章为绪论，介绍了本课题的背景及研究意义，阐述了图像加密技术的发展历程 及技术特点。随后介绍了国内外对图像加密算法的设计与改进方案，主要包括提升算法 中所应用混沌系统的性能以及改进加密机制。

第 2 章详细介绍了与本文研究课题相关的理论与技术基础，即混沌理论与图像加密 技术。具体阐述了混沌系统的定义、特点、性能测试方案以及几种常见的混沌系统，还 介绍了一些常见的混沌图像加密机制，为后文的研究工作提供基础理论知识。

第 3 章提出了一种基于无平衡点混沌系统的混沌魔方变换图像加密算法。首先， 通 过在三维混沌系统中引入一个附加变量和一个常数项，构造了一个新的非平衡混沌系统。 然后利用所提出的混沌系统，提出了一种具有经典排列-扩散结构的混沌魔方变换图像 加密算法（CMCT-IEA）。该算法中设计了一种新的排列方法来打乱三维空间中的图像像 素，并提出了一种扩散方法来将原始图像微小的像素变化扩散到三维空间中的所有像素。 为了提高加密算法的安全性，还设计了动态密钥。最后，我们还从计算复杂性、统计特 性和防御几种常见攻击的能力方面分析了 CMCT-IEA 的安全性。与几种先进的算法相 比，CMCT-IEA 具有优良的安全特性。

第 4 章提出了一种基于 2D-Price 混沌映射的同步置乱-扩散图像加密算法。首先， 基于经典的 Price 映射提出了一种新的二维 Price 混沌映射，对其性能分析表明所提出的 系统具备更好的混沌动力学特性。然后，本文利用二维 Price 混沌系统设计了一种基于 索引的同步置乱-扩散图像加密算法（ISPD-IEA）。ISPD-IEA 将传统的置乱与扩散过程 结合为一个整体，使其在加密图像的过程中能够同时进行像素位置的改变与像素变化的 扩散工作，因此所设计的算法在拥有良好安全性能的同时还具备并且极高的加密效率。

第 5 章设计了一种忆阻超混沌正弦映射的图像加密算法（MHSM-IEA）。首先，将 一维 Sine 混沌系统与一个忆阻器进行耦合得到一个新的二维忆阻耦合超混沌映射（2D-

5

中国知网 https:iiwww.cnki . net

MHSM），并且该系统并原系统表现出了更复杂的动力学行为。随后，基于 2D-MHSM 设 计了一种具有高安全性的图像加密算法。该算法包含了置乱与扩散两个部分， 前者能够 使数字图像的像素排列变得无序，后者则借助了一种基于比特的双环移位异或机制将原 始图像的微小变化传播到整个密码图像并改变图像的像素值。最后， 对提出算法的加解 密效果进行仿真研究，结果表明该算法具有极其可靠的安全性能。

第 6 章对本文所研究的内容进行了归纳与总结，同时对图像加密算法的设计研究进 行了展望。

6

中国知网 https:iiwww.cnki . net

**第二章** **混沌理论与图像加密基础**

**2.1** **混沌理论**

混沌是一种广泛存在于自然界中的物理现象，其特性为能够在确定条件下表现出非 线性的伪随机效应。1963 年，美国气象学家洛伦兹首次证实了混沌现象客观地存在于自 然界中，并提出了广为人知的“蝴蝶效应”。随着研究的深入， 混沌的优良特性在诸多领 域得到了广泛应用，如区块链经济、信息安全、半导体电子以及航空航天等。因此， 混 沌理论能够与量子力学、相对论并称为二十世纪最具影响力的三大发现[55]，人们对其探 究的脚步也从未停止。

**2.1.1 混沌的定义及特点**

1975 年，华裔学者 Li T. Y.与其老师 J. A. Yorke 首次对混沌进行了数学层次上的分 析进而总结出“周期三即混沌”，并提出了著名的 Li-Yorke 定义，这也是迄今为止最具 认同性的混沌定义。Li-Yorke 定义具体描述如下 [56] ：

对于闭区间 L 上的连续自映射f(x)，且其周期点的周期无上界，若闭区间 L 中存在 满足以下 3 点条件的不可数子集 S，则存在混沌现象。

（1）对于任意 x, y ∈ S ，当 x ≠ y 时，有

lim supl f n (x)  f n (y)l >0 (2-1)

n  oo

（2）对于任意 x, y ∈ S ，有

lim inf f" (x)  f " (y) l   (2-2)

n  oo

（3）对于任意x, y ∈ S ，当 y 是 f 的任意一周期点，则有

lim sup lf " (x)  f " (y) l > 0 (2-3)

n → 

由上述定义可知，混沌系统能够在有限区间内进行极其复杂的非线性行为。其主要 特征包括以下几个方面[57]：

1. 有界性：混沌运动虽是复杂且无规律的，但其运动轨迹始终局限于一个确定区域， 即混沌吸引域。

2. 遍历性：混沌运动轨迹能够在有限的时间内经过所在混沌吸引域内的所有状态值。

3. 内随机性：在初始状态确定时，混沌运动所表现出的随机性只由系统的内部决定， 不受外界的影响。

4. 初始状态敏感性：混沌运动对初始的状态值极其敏感，对于同一个混沌系统而言， 即使初始状态值发生了细微的变化，最终所对应的运动轨迹也将截然不同。

5. 长期不可预测性：混沌系统的混沌动力学行为由混沌系统对初初始条件极端敏感

7

中国知网 https:iiwww.cnki . net

的特性所决定，具备长期不可预测性。

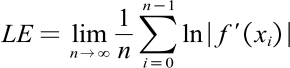
6. 普适性：混沌系统所具备的特性是其内在规律的体现，不会随动力方程或参数的 变化而改变。

**2.1.2 混沌系统的判定标准**

混沌所具备的普适性致使混沌系统的动力学方程形式多样，因此混沌系统的判定工 作备受关注。当前可通过一些数学方式对混沌特性进行定性与定量分析，常用的判定方 法有以下几种：

（1）Lyapunov 指数法[58] 。对初始条件极其敏感是混沌系统异于其他系统的显著特

征。Lyapunov 指数（*LE*）是测定系统是否具备混沌特性的重要指标，它不仅能定性地判 断系统是否对初始条件敏感，还能定量地衡量系统对初始条件的敏感程度。其定义为两 个差异极小的初始状态值分别在系统内的运行，随着时间的推移它们的运动轨迹之间的 平均偏移率。以一个可微的一维动力系统xn  i  F(xn)为例，其对应的 *LE* 可由下式所 得：

 (2-4)

对于系统xn  i  F(xn) ，当 LE < 0 时，此时系统运动轨道呈收缩状态，系统是稳定 的；当LE  0 时，此时系统处于临界稳定状态；当LE > 0 时，此时系统运动轨道呈发 散状态，系统处于混沌状态。另外，*LE* 的大小可反映出对应系统混沌特性的强弱程度， 一般 *LE* 越大，混沌特性越强。对于高维动力系统，只要存在大于 0 的 *LE* 值，该系统则 可被认为是混沌的。如果一个系统存在数量为两个或两个以上正的 *LE* 值，那么该系统 便被认为是比混沌系统具备更复杂动力学行为的超混沌系统。

（2）相图描述法。相空间主要用于描述系统状态变量随时间产生的变化情况，是研 究混沌系统常用的方法之一。系统相空间的维度与其状态变量的数量一致。相空间内所 包含的所有相点为系统随时间所得到的状态值，由所有状态变量共同作用生成，并且它 们共同构成的运动轨迹即为系统的相图。对于一个稳定系统，其相图呈现为一系列相对 孤立的点；对于一个周期系统，其相图则表现为简单的闭合曲线；而对于混沌系统，其 相图在相空间内呈现为结构复杂的曲线。

（3）Kolmogorov 熵判定法。Kolmogorov 熵（*KE*）用于描述动力系统状态演化的混 乱程度。它通过测试使用先前状态预测未来轨迹所需的额外信息来评估混沌程度。对于 一个 *n* 维动力系统，将其所具备的 *n* 维相空间均分为*n*+1 个大小为  的子空间，各子空 间分别为io , i ,i2 · · · · · · , in ，该动力系统的 *KE* 值可由下式求得：



其中，*n* 是系统的维度， T 为时间间隔，假设系统的运动轨迹的初始起点为 i, ，则

8

中国知网 https:iiwww.cnki . net

p(i ,i2 …,in)代表当时间为T 时系统轨迹在子空间i ,i2,…,in 内的联合概率。对于任意 *KE* 值为正数的动力系统，需寻求额外信息方可预测其运动轨迹，因此该系统可被认为时不 可预测的，并且系统的不可预测性和状态演化的混乱程度与 *KE* 值成正比关系。

（4）分岔图。动力系统在其系统参数变化至某个临界数值时所对应的状态轨迹突 然产生变化，这一现象被称为分岔。描述分岔现象的图形即为分岔图， 一般来说，分岔 图能通过计算在不同系统参数或初始状态情况下时域图中的极大值来获得。当系统参数 或初始状态改变时，分岔图能够清晰地反应系统状态的动态变化，也能反映出系统通向 混沌的路径。

**2.1.3 几种常见的混沌系统**

1. Sine 映射

Sine 混沌映射因具备极为简单的组成结构使其成为最常见的混沌系统之一。其数学 定义如下：

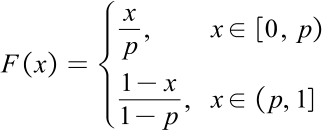
xi  i  μ · sin(m · xi) (2-6) 其中，  为混沌参数，并且uc [0, 1] ，xi 为迭代i 次的混沌值，xi i i 为迭代i  1 次对应 的混沌值。

2. Logistic 映射：

xi  1  K · xi (1  xi) (2-7)

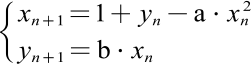
当3 . 569945627 <  < 4 时，该映射处于混沌状态。

3. Tent 映射：

 (2-8)

其中，p  0 . 5 。

4. Henon 映射：

 (2-9)

其中，当参数a  1 . 4 ，b  0 . 3 时，该映射处于混沌状态。

5. Arnold 映射：

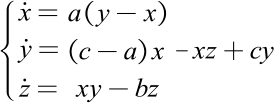
 (2-10)

其中，a 和b 为实数，xn , yn o , 1) 。

9

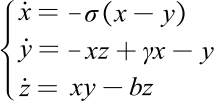
中国知网 https:iiwww.cnki . net

6. Chen 系统：

 (2-11)

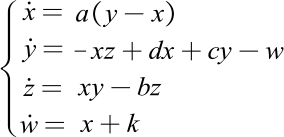
其中，*x*, *y*, *z* 为状态变量，当参数      时，系统处于混沌状态。

7. Lorenz 系统：

 (2-12)

其中，  ,  ,  为状态变量，当参数          或          时， 系统处于混沌状态。

8. Chen 超混沌系统：

 (2-13)

其中，*x*, *y*, *z*, *w* 为状态变量，当参数    ，   ，        [-0.7,0.7]时， 系统处于超混沌状态。

混沌系统在其处于混沌状态时能够表现出独有的混沌特性。以 Henon 映射为例，其 表达式如式(2-9)所示，分别令其初始状态值    ，   ，参数    ，   ， 此时，Henon 映射的相空间图如图 2-1 所示。另外，取   ，   ， ，    , 图 2-2 展示该映射的分岔图，图 2-3 则为该映射的 Lyapunov 指数。

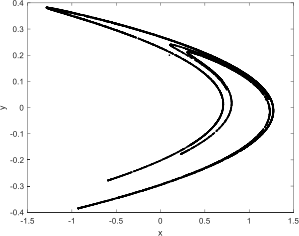


图 2-1 Henon 映射混沌吸引子图

Fig. 2-1 The chaotic attractor diagram of Henon map

10

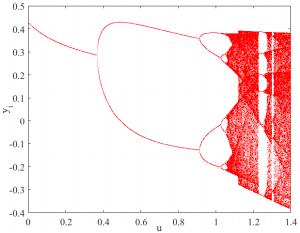
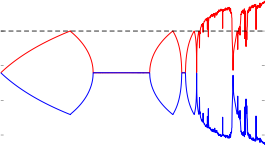


图 2-2 Henon 映射的分岔图

Fig. 2-2 The bifurcation diagram of Henon map

|  |  |
| --- | --- |
|  | 入1  入2 |
|  | |

a

图 2-3 Henon 映射的 Lyapunov 指数图

Fig. 2-3 The lyapunov exponent diagram of Henon map

由图 2-1 可知，Henon 映射的各状态值在相空间内的运动轨迹较为复杂并且无明显 规律，符合混沌系统所具备的特点。结合图 2-2 与图 2-3 可以看出：若 *LE* 值为负值，系 统无混沌行为；若 *LE* 值为 0 时，系统处于临界状态且存在周期分岔点；若 *LE* 值为正 值，系统处于混沌状态。

**2.2** **密码学基础知识**

密码学是一种研究信息安全的重要学科[59]。人类对密码的使用历史源远流长，从古 代战争中军队内部的机密信件到近现代历史中所使用的电报，再到如今数字时代随处可 见的账户密码等，无不体现出密码学对于人类生活的极大作用。一般地，密码学包含了 两个主要内容：密码编码学与密码分析学。其中，前者主要是通过研究加密策略进而将 信息数据转变为无法识别的密文信息，而后者的主要是进行密码系统的安全性分析以及 密文信息的破译工作，并且二者之间存在着一种“博弈”关系。因此， 密码学的发展离

11

中国知网 https:iiwww.cnki . net

不开密码编码与密码分析之间的掣肘。

**2.2.1 密码编码学**

密码编码学通过研究加密策略并设计出可靠的密码系统，进而实现对数据信息的加 密保护工作。如图 2-4 所示，一个完整的密码系统应至少包含加密系统、密钥、解密系 统以及通信信道等部分。密码系统的具体运行过程为：首先，明文信息与密钥作为输入， 在加密系统的作用下生成密文信息；随后，密文信息经公共信道传递至解密系统，同时， 密钥通过私密信道传递至解密系统；最后，密文信息与密钥作为输入，在解密系统的作 用下完成解密，获得解密结果。

|  |  |  |
| --- | --- | --- |
| 密钥 | 私密信道 | 密钥 |
|  |

明文信息

解密结果

|  |  |  |
| --- | --- | --- |
| **加密系统** | 密文信息 | **解密系统** |
| 公共信道 |

图 2-4 密码系统的运行过程

Fig. 2-4 The operation process of the cryptographic system

一般地，密码系统的类型可根据以下三个方面进行区分：

1. 明文信息的加密形式。密码系统对明文信息的加密形式主要有两种：流加密与分 组加密。其中， 流加密是将明文中的信息转换为二进制流后再进行加密运算，而分组加 密则是先将明文信息进行分组操作，再对所有的信息组进行加密处理。

2. 加密体制。加密体制由两部分组成：对称加密体制与非对称加密体制。前者的加、 解密机制是对称的，因此其加密与解密过程之间互为可逆关系，并且共用同一密钥。而 后者的加、解密机制是非对称的，其密钥分为公钥与私钥。一般地，加密方使用公钥加 密明文，而解密方则使用配套的私钥对密文实现解密。

3. 加密的操作方式。密码系统加密明文信息时一般采用置乱与扩散两种操作方式。 其中，前者主要是改变明文信息的排列位置，而后者则是改变明文信息的表现形态。

**2.2.2 密码分析学**

密码分析学主要用于分析密码系统的安全性， 也可用于破译密文信息。 根据 Kerckhoffs 准则[60]，常见的密码分析攻击方法主要有以下四种：

1. 唯密文攻击：攻击者根据密文信息直接进行破译工作。

2. 已知明文攻击：攻击者获取了明文信息以及对应的部分密文信息，进而分析密码 系统并获取密钥。

12

中国知网 https:iiwww.cnki . net

3. 选择明文攻击：在知悉密码系统加密机制的前提下，攻击者能够选取特定的明文 信息进行加密操作，并且能够获取对应的密文信息，进而分析密码系统并获取密钥。

4. 选择密文攻击：在知悉密码系统解密机制的前提下，攻击者能够选取特定的密文 信息进行解密操作，并且能够获取对应的明文信息，进而分析密码系统并获取密钥。

以上四种密码系统分析攻击方法中，分析、破译难度最小的方法为选择明文攻击。 因此，一个密码系统倘若具备抵御选择明文攻击的能力，则表明其也能够抵御其它三种 分析攻击方法。此外，一些攻击者还可使用穷举法和统计分析法来攻击密码系统。其中， 穷举法主要是尝试利用所有的潜在密钥对密码系统进行暴力破译，而统计分析法则是通 过计算密文的统计学特性进而分析出相关明文信息。

**2.3** **混沌图像加密基础**

**2.3.1 混沌理论与密码学的联系**

科技的不断进步使得如今计算机设备拥有了更强的数据分析能力，这导致传统的数 字密码系统的安全性能日渐式微。为寻求一种更安全的数字信息加密方法，众多研究者 一直以来都在不断地探索与尝试，混沌系统因其具备的优异特性逐渐引起了他们的注意。

研究人员发现混沌系统与密码系统之间存在许多相似之处。例如， 密码系统加密任 意明文信息所得的密文信息都十分相似，这与混沌系统的遍历性特点相似；密码系统加 密的密钥发生微小变化会导致加密结果产生巨大变化，这与混沌系统的初始参数极端敏 感特性相似。另外， 著名密码学家 Shanon 早在 1949 年便指出设计密码系统的两个基本 原则：混淆与扩散[59]。其中，混淆主要是将明文信息进行无差别置乱使其加密前后之间 无统计信息关系；扩散则是将明文信息的微小变化尽可能传递至密文信息全局，进而拥 有较好的抵御差分攻击能力。这与混沌系统在相空间内的拓扑传递与混迭特性。

近几年，许多学者将混沌理论与密码学结合进而设计出大量的混沌密码算法，这些 算法大致可分为两类加密策略：一类是将混沌系统生成的具有为随机性的混沌序列作为 加密过程的序列密码；另一类则是将明文信息作为混沌系统的初始条件，经迭代多次后 得到密文信息。

**2.3.2 混沌图像加密技术**

数字图像加密技术可以把图像转换为类似噪声图像进行传输，并且能够将加密后的 图片恢复如初。数字图像的加密原理为：将数字图像视为与其尺寸大小相同的像素矩阵， 由于图像的内容随着像素的变化而改变，因此图像加密可被视为如何改变图像像素位置 与像素值的问题。

混沌数字图像加密技术由混沌密码学与数字图像加密技术结合所得，利用混沌序列 发生器（混沌系统）生成的混沌序列对明文图像在像素平面或位平面进行置乱、扩散操 作，进而改变明文密图像的像素状况，最终完成对图像加密工作。下面简要地介绍几种

13

中国知网 https:iiwww.cnki . net

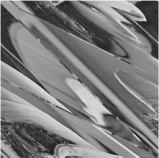
常见的基于混沌的置乱与扩散方法。

（1）基于混沌的置乱方法

① Arnold 置乱法：对于尺寸为M  M 的明文图像，将图像视作尺寸为M  M 的像 素矩阵，随后再根据式(2-14)所示的 Arnold 映射改变明文图像中所有像素的位置。

 (2-14)

其中，*x*、*y* 分别为明文图像的像素横、纵坐标，x ' 、y ' 分别为密文图像的像素横、纵坐 标，M 为矩阵尺寸数。以尺寸为256  256 的“Lena ”图像作为明文图像，利用式(2-14) 所示的 Arnold 映射对明文图像进行两次置乱操作，所得结果如图2-5 所示。



(a) 明文图像 (b) 置乱结果

图 2-5 Arnold 映射置乱

Fig. 2-5 The permutation of Arnold map

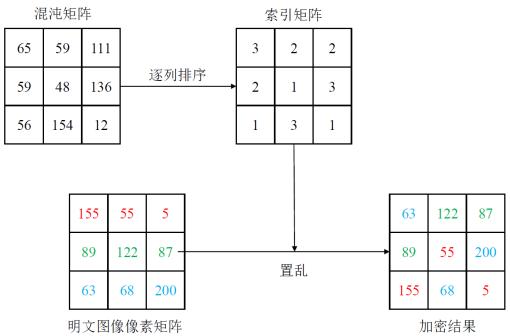


图 2-6 基于混沌序列的索引置乱图例

Fig. 2-6 Example of index permutation based on chaotic sequences

14

中国知网 https:iiwww.cnki . net

② 混沌索引置乱法：将混沌序列转换成与原始图像尺寸大小相同的矩阵得到相应 的混沌矩阵，对混沌矩阵逐行/列的序列值降序（升序）排列，获得索引矩阵，然后将原 始图像的像素依据索引矩阵进行排列。图 2-6 提供了一个基于混沌序列的索引置乱图例。

如图 2-6 所示，首先，将混沌矩阵的各列混沌值按数值大小进行降序排列，获取相 应的索引矩阵。然后，根据索引矩阵，改变原图像素矩阵对应坐标位置的像素排列方式， 以第一列像素置乱过程为例，索引矩阵坐标为(1,1)的索引顺序为“3 ”，因此原图像素矩 阵中坐标为(1,1)的像素移动至该列从上至下的第 3 个位置，再以相同的变换方式变换该 列的其它像素。最后，对所有列依次进行置乱操作后可得到加密结果。

（2）基于混沌的扩散方法

① 直接运算法：首先，将明文图像视为一个像素矩阵，利用混沌系统一个与像素矩 阵大小相同的混沌矩阵；然后，对混沌矩阵中所有的元素进行放大、取整以及取模运算 得到一个随机混沌矩阵；最后，将随机混沌矩阵与像素矩阵之间进行加和、取模或者异 或等运算，得到加密结果。

② DNA 编码与序列运算法：将图像像素与混沌序列分别进行 DNA 编码操作，再 将它们的编码结果进行相应的运算，完成扩散操作。

DNA 包括四种核苷酸，即腺嘌呤（A）、胸腺嘧啶（T）、胞嘧啶（C）和鸟嘌呤（G）， 其中 A 与 T ，C 与 G 分别成对互补，这与比特数“0”与“1”之间的互补关系十分相 似，并且“00”与“11”，“01”与“10”也分别成对互补。因此，A、T、C、G 可用“00”、 “ 11”、“01”、“10 ”进行编码，由于 A 与 T ，C 与T 之间存在互补关系，最终可设置出 8 种不同的编码规则，具体的编码方式如表 1-1 所示。以像素值 158 为例，先将其转换 为二进制序列即“10011110 ”，利用表 1-1 所示的 8 种编码规则分别对该序列编码可得到 相应的编码结果，规则 1：“GCTG”，规则 2：“CGTC”，规则 3：“GCAG”，规则 4 ： “CGAC”，规则 5：“ATGA”，规则 6：“TACT”，规则 7：“ATCA”，规则 8：“TAGT ”。 同理，利用表 1-1 的编码规则也可对整数型混沌值进行编码操作。编码后的像素值与混 沌值可基于传统的二进制运算进行 DNA 运算，得到加密结果。假设选取“规则 1 ”为编 码规则，其加法运算规则如表 1-2 所示，此外，编码之间也可进行减法、同或以及异或 运算。

表 1-1 DNA 编码规则

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

表 1-2 DNA 加法运算规则

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

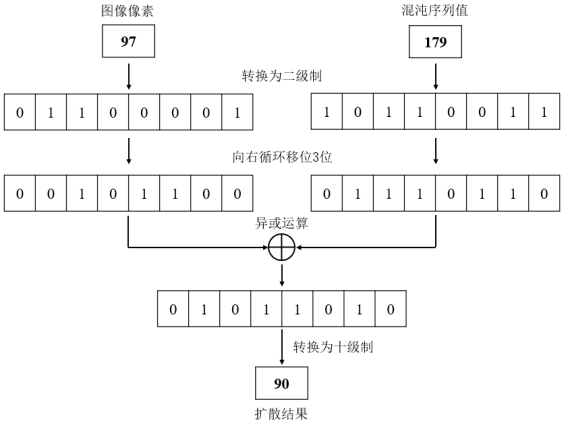


图 2-7 循环位移与序列运算图例

Fig. 2-7 Example of cyclic shift and sequence operations

③ 循环位移与序列运算法：将各图像像素值与混沌序列值转换成 8 位二进制值序 列，然后改变二进制值在序列中的排列位置，最后再将图像像素值与混沌序列值所对应 的序列进行各类运算。以上过程可通过图 2-7 提供的示例所示。

以上所述的置乱与扩散方法均具有可逆性，符合图像加密系统的解密需求。

**2.3.3 混沌图像加密算法的设计**

由以上所述的混沌与图像加密理论知识可知，在设计混沌图像加密算法时需对以下 几个方面进行考虑[61]。

（1）选取具备优异动力学特性的混沌系统：当前设备的计算精度无法达到理想条 件，这使得系统在仿真测试中可能出现混沌退化以及短周期性等问题。因此， 在设计混

沌图像加密算法时，应确保所选择的混沌系统具备稳定、优异的混沌动力学特性。

（2）安全评估：传统的文本信息加密系统经长期发展已形成了较为全面的安全评 估体系。当前， 混沌图像加密系统的安全评估体系还不够成熟，需借助一些其它量化指 标对其安全性进行评估。因此， 在设计混沌图像加密算法时需保证其能够通过各类安全 测试。

（3）加密效率：为追求较高的安全性，研究人员在设计图像加密系统时通常会提高 加密算法的复杂度或增加加密轮数，所设计出的加密系统往往拥有较低的加密效率。数 字图像所包含的信息量远超过传统的文本载体，因此，在设计混沌图像加密系统时，应 尽可能处理好算法安全性与加密效率之间的平衡关系，使得加密算法在拥有良好安全性 同时也具备良好的加密效率。

结合以上所述内容，可根据以下步骤设计混沌图像加密算法：

步骤一：选择混沌动力学特性良好的混沌系统，若选取的混沌系统为连续系统，则 需对其进行离散化处理。

步骤二：结合混沌系统的初始条件（初始状态值，混沌参数）设计出加密系统的密 钥，确保加密密钥拥有良好的敏感性与足够大的空间。

步骤三：以密码学与图像加密技术为基础，并利用混沌系统设计出高效、安全的加 密机制。

步骤四：加密算法的解密机制与加密机制之间应具有可逆性。

步骤五：在确保加密算法能够对图像完成加密与解密的前提下，还须通过各项安全 性能测试。

**2.4** **本章小结**

本章介绍了混沌图像加密算法的主要研究内容：混沌理论、密码学以及混沌图像加 密技术。首先， 介绍了混沌的定义特点以及混沌系统的相关性能指标，并列举了一些常 见的混沌系统以供参考。其次， 对密码学领域内的基础知识进行介绍。最后， 介绍了一 些经典的图像加密算法设计方案以及相应的性能评估指标。通过对以上相关理论基础知 识的介绍，为后文混沌系统以及图像加密机制的改进、设计工作提供理论支持。

17

中国知网 https:iiwww.cnki . net

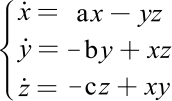
**第三章** **基于无平衡点混沌系统的混沌魔方变换图像加密算法**

针对当前有许多的混沌图像加密算法中存在混沌系统结构简单、混沌区间小与加密 机制过于简单等问题，本章提出了一种基于无平衡点混沌系统的混沌魔方变换图像加密 算法（CMCT-IEA）。首先，基于现有的一个三维混沌系统，通过引入一个变量和两个常 数项生成一个新的无平衡点混沌系统，并且该系统具有倍周期分岔并且在较大的常数项 范围内具有隐藏混沌吸引子。然后，利用无平衡点混沌系统生成的混沌序列在三维空间 内完成对明文图像像素的置乱与扩散工作。最后，安全仿真测试结果表明，CMCT-IEA 在拥有良好安全性的同时还具备较高的加密效率。

**3.1** **无平衡点混沌系统的设计与分析**

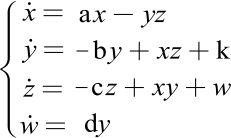
本节通过在一个三维混沌系统中引入一个附加变量和一个常数项，构造了一个新的 非平衡混沌系统，并给出了新的无平衡系统的分岔图和 Lyapunov 指数。

对于一个三维连续自治混沌系统如式(3-1)所示：

 (3-1)

其中，x, y, Z 为状态变量，a, b, C 为系统参数。该系统在a > 0 , b > 0 , C > 0 时存在多 个平衡点，并且能够很容易地生成多卷波奇异吸引子。

本文根据式(3-1)所示的混沌系统构造了一个新的无平衡点混沌系统，通过增加一个 新的变量 *w* 以及对应的变量参数 d 、一个大于 0 的常数相 k ，使得原混沌系统扩展为一 个新的四维混沌系统，所得系统如下式所示：

 (3-2)

其中，x, y, z, W 为状态变量，a, b, C, d, k 为系统参数，当a < b  ~~I~~  C 时，系统是耗散的。 取x·  y·  Z·  w·   , a  4 , b  16 , C  10 , k  50 ，再令系统参数d  [s,16 ，该系统 的分岔图与 Lyapunov 指数（*LE*）如图 3-1 ，3-2 所示。其中, 图 3-1 为混沌系统的分岔 图，图 3-2 给出了 3 个 *LE* 值Li 、L2 、L3 ，该系统最小的一个 *LE* 值L4 < - 10 。令参数 d 的取值分别为 8 、10 、11.5 、12.8，获取该系统的 4 个隐藏周期分别为周期 1、周期 2 、 周期 3、周期 4 ，它们所对应的混沌吸引子如图 3-3 所示。图 3-4 为该系统在参数 a  4 , b  16 , C  10 , d  16 , k  56 且各状态值取x·  y·  Z·  W·   时产生的隐藏

18

中国知网 https:iiwww.cnki . net

混沌吸引子图，此时对应的 *LE* 值L1  0 . 3505 ，系统处于混沌状态。

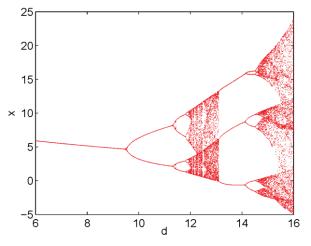


图 3-1 所提出的无平衡点混沌系统分岔图

Fig. 3-1 The bifurcation diagram of the proposed no-equilibrium chaotic system

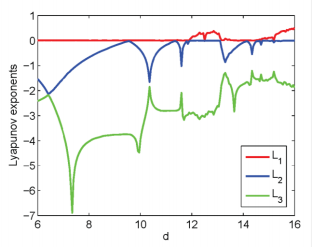


图 3-2 所提出的无平衡点混沌系统 Lyapunov 指数图

Fig. 3-2 The lyapunov exponent diagram of the proposed no-equilibrium chaotic system

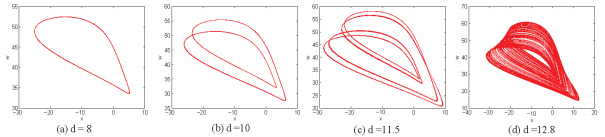


图 3-3 所提出的无平衡点混沌系统分别在 d = 8, d = 10, d = 11.5, d = 12.8 对应的隐藏周期混沌吸子

Fig. 3-3 Hidden chaotic attractor of the proposed no-equilibrium chaotic system with

d = 8, d = 10, d = 11.5, d = 12.8 respectively

19

中国知网 https:iiwww.cnki . net

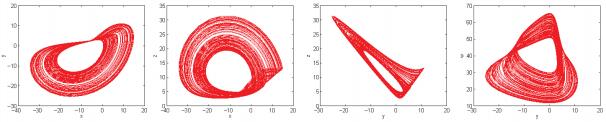


图 3-4 所提出无平衡点混沌系统在 k = 56, a = 4, b =16, c = 10, d =16 时的隐藏混沌吸引子

Fig. 3-4 Hidden chaotic attractor of the proposed no-equilibrium chaotic system

with k = 56, a = 4, b =16, c = 10, d =16

表 3-1 本文所提出混沌系统生成的二进制序列的 NIST SP800-22 测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| 子测试 | | P 值 | 结果 |
| 单比特频率 | | 0.1550 | 通过 |
| 频率块 | | 0.3953 | 通过 |
| 游程 | | 0.3607 | 通过 |
| 最长游程 | | 0.1652 | 通过 |
| 二进制矩阵秩 | | 0.0143 | 通过 |
| 离散傅氏变换 | | 0.2701 | 通过 |
| 非重叠模板匹配 | | 0.5465 | 通过 |
| 重叠模板匹配 | | 0.8615 | 通过 |
| 通用统计 | | 0.7610 | 通过 |
| 线性复杂度 | | 0.6707 | 通过 |
| 随机游动 | | 0.4674 | 通过 |
| 随机游动状态频数 | | 0.2117 | 通过 |
| 近似熵 | | 0.0191 | 通过 |
| 序列测试 | P 值 1 | 0.1740 | 通过 |
| P 值 2 | 0.7279 | 通过 |
| 累加和 | 正向 | 0.4911 | 通过 |
| 反向 | 0.3476 | 通过 |

为了进一步说明本章所设计的无平衡点混沌系统适用于图像加密方案的设计工作， 根据美国国家标准与技术研究院(NIST) SP800-22[62]对所提出的无平衡点混沌系统输出 序列的随机性进行测试。为了执行该测试，需要将混沌系统生成混沌序列转换成二进制 序列，并依次作为测试的输入项。该测试有 15 个子测试结果（P 值），并且所有的测试 结果都应该在 0.01 到 1 之间。本文使用该混沌系统生成的长度为 100 万的二进制序列 作为测试输入，得到的测试结果如表 3-1 所示。可以看出， 本章所设计的无平衡点混沌

系统生成的二进制序列通过了所有子测试，这意味着该系统能够满足图像加密的要求。

**3.2** **图像加密算法介绍**

基于上述的四维无平衡点混沌系统，本文设计了一个基于无平衡点混沌系统的混沌 魔方变换图像加密算法（CMCT-IEA），图 3-5 展示了该算法的加密流程。由图 3-5 可知， 明文图像经预处理后可得到三维魔方像素矩阵以及密钥。然后，将密钥作用于无平衡点 混沌系统，得到相应的混沌序列，再将混沌序列转换为三维魔方混沌矩阵。最后， 在密 钥的作用下，三维魔方像素矩阵与三维魔方混沌矩阵经三轮置乱、扩散操作后得到密文 图像。

|  |
| --- |
| 密钥 |

|  |
| --- |
| 预处理 |

|  |
| --- |
| 三维魔方像素矩阵 |

|  |
| --- |
| 置乱操作 |

|  |
| --- |
| 扩散操作 |

▲

|  |
| --- |
| 三维魔方混沌矩阵 |

|  |
| --- |
| 明文图像 |

|  |
| --- |
| 无平衡点混沌系统 |

|  |
| --- |
| 混沌序列 |

|  |
| --- |
| 密文图像 |

循环3轮

图 3-5 CMCT-IEA 加密结构

Fig. 3-5 The encryption structure of CMCT-IEA

**3.2.1 算法的加密过程**

（1）预处理过程

由图 3-5 可知， 明文图像经预处理过程后得到三维魔方像素矩阵，对于尺寸为 M  N 的明文图像 *P*，预处理过程如下。① 计算明文图像的像素总量S  M  N ，随后 计算b,  3  S ，如果bo 是一个整数，取b,  bo ，否则，bi 为bo 向上取整后的值；② 建立 一个尺寸为b,xb,xb, 的三维空矩阵，随后将明文图像的像素依次填充至该三维空矩阵； ③ 若三维空矩阵未被图像像素充满，则额外补充数量为bi3  S 的像素，且补充的像素的 数值范围为[0, 255]；最终获得了一个尺寸为b1xb1xb, 的三维魔方像素矩阵。

（2）密钥设计

密钥对于一个加密系统而言至关重要。本文所设计的图像加密算法的密钥由预处理

21

中国知网 https:iiwww.cnki . net

中的计算结果、混沌系统的参数以及明文图像的尺寸等三个部分组成。首先，根据预处 理所得的结果bi ，随机生成长度为3  bi 的二进制数组ki ，并将ki作为密钥的第一部分。 其次，将该算法中所选用的无平衡点混沌系统的初始参数作为密钥的第二部分。最后， 将明文的行与列对应的数值M 、N 作为密钥的第三部分。另外，密钥的第一部分与第二 部分皆可根据加密者的需求进行设定，并非固定数值。

（3）三维魔方混沌矩阵的生成

根据图 3-5，无平衡点混沌系统可根据密钥第一部分所提供的信息生成混沌序列。 首先，将密钥中所有的整数值进行求和，所得结果为 *h* 。随后，将密钥中的第二部分作 为混沌系统的初始参数 。 然后 ， 利用混沌系统得到四组足够长的混沌序列 {X, Y, Z , W} ，再分别从xi 、yi 与zi 中的选取三组长度为bi3 的混沌序列组，并且选 取序列的起始位置为第 *h* 位。最后，再将上述选取的三组混沌序列分别转换为尺寸为 b,  b,  bi 的三维混沌魔方矩阵si 、S2 、与 s3 。

（4）置乱过程

大多数数字图像中相邻的像素之间具有紧密的关联性，这使得攻击者有可能从这些 图像中窃取信息。因此， 在制定图像加密策略时，需尽可能地将图像所有像素的排列位 置变得混乱。常用的置乱算法主要是对二维图像像素矩阵的行、列的像素进行一些加密 操作。本章从魔方玩具中获取灵感，设计了一种在三维空间中对图像像素位置进行无序 化处理的方法，利用加密密钥作为三维魔方像素矩阵中的像素平面矩阵的操作指令，随 后再利用三维魔方混沌矩阵中对应位置的混沌序列对各像素平面矩阵进行置乱操作。下 面详细介绍算法的置乱过程：

步骤 1 ：初始图像经预处理过程后得到一个尺寸为  的三维魔方像素矩阵 P ，并且由无平衡点混沌系统生成的混沌序列也被转换为尺寸为b1xb1×b, 的三维魔方 混沌矩阵S 。

步骤 2：获取密钥的第一部分即二进制数组ki ，首先读取ki 中的第i(i  1)位二进制 数并将该二进制数作为三维魔方像素矩阵pi 中像素平面p  pi (: , 1 , :) 的操作指令，具体 为：若该二进制数为“ 1 ”，将像素平面*p* 按顺时针旋转 90 度；否则，将该像素平面翻 折。

步骤 3：从三维魔方混沌矩阵S 中选取一个混沌平面si ，其中si 在S 中的位置与*p* 在 pi 中的位置相同，因此si  S(: , 1 , :) 。随后，分别将 *p* 与si 进行重组，进而获得一维行 向量vi 、v2 ，它们的尺寸均为  bi2 。

步骤 4 ：将向量v2 中的混沌序列按数值从小到大进行排序，获得索引向量o 。

步骤 5：从向量vi 中选取图像像素并且被选取像素对应的位置为{(1,0.i) , (1 , oi · 2 .(1,0i 2)} ，将选取的像素重组为一个尺寸为b,  b 的二维像素矩阵p2 ，随后将原来p 中*p* 替换为p2 。

22

中国知网 https:iiwww.cnki . net

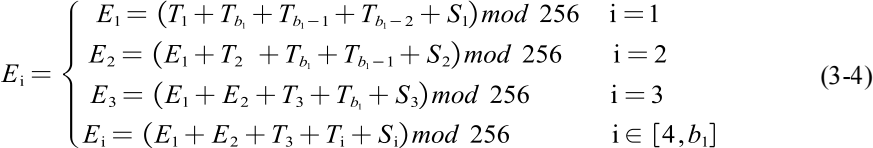
步骤 6：重复进行步骤 2 ~ 5。每次运行步骤 2 时，依次读取ki 的第j  2 , 3,…, 3  bi 位二进制数，其中，当j  3  i  2(i  2 , 3,…,b) 时，P  P, (i, : , :) ；当j  3  i  1(i  2 , 3,…,b)时，p  P (: , i, :) ；当j  3  i(i  2 , 3,…,b)时，p  P (:,:,i)。最终得到置 乱后的三维魔方像素矩阵T 。

为了更好地解释置乱过程，我们以一幅尺寸大小为5x5 的数字图像作为示例，具体 过程如图3-6 所示。明文图像经预处理后得到密钥以及三维魔法像素矩阵pi ，其中，密 钥中第一部分所含的二进制数长度为 9 位，魔方块“26 ”和“27 ”由随机数补充，并且 补充魔方的值范围为 0 到 255 。利用三维魔方混沌矩阵S 对pi进行置乱操作。置乱过程 为：假设读取密钥的第一位结果是“1”，则选取pi 中的一个像素平面p  P (:, 1, :)，先将 *p* 按顺时针方向旋转90- ，再将旋转后的*p* 重组得到一个大小为1  9 的一维像素矩阵v2 ， 与此同时，从三维魔方混沌矩阵S 中选取对应位置的一个混沌平面si  S(: , 1 , : ) 并将si 重组得到一个大小为1  9 的一维混沌矩阵V2 。将V2 中的混沌值按数值大小实施升序排列 操作，获取索引向量o 。根据索引向量。将vi 中的像素重新排列，随后再重组成大小为 3  3 的像素矩阵p2并取代pi 中的*p*。然后，依次读取密钥中剩余的 8 个二进制数，并依 据步骤 6 以及上述过程完成置乱操作，最终得到三维魔方像素矩阵 *T*。

（5）扩散过程

在本课题设计的加密算法扩散机制中，将置乱后的三维魔方像素矩阵作为输入，在 三维魔方混沌矩阵与三维魔方像素矩阵之间采取加和、取模等方式来改变所有的像素值。 假设 *T* 为置乱操作后所得的三维魔方像素矩阵，*S* 为三维魔方混沌矩阵，并且他们的尺 寸大小均为b1xb1xb, 。首先，对 *S* 中所有的混沌序列值进行放大、向下取整操作，具 体过程如式(3-3)所示，其中floor(:)为向下取整指令。 随后，利用放大、取整后的 *S* 对 *T* 进行扩散操作，扩散操作的具体过程如式(3-4)所示。

S  floor (s  224 ) (3-3)



其 中 ，m,:d 为取模操作， 扩散操作选取的操作对象为 *S* 与 *T* 的每个二维平面即

si S(i, , :) ，Ti T(i, : , :) 。最终，完成扩散操作后得到新的三维魔方像素矩阵 *E*。

23

中国知网 https:iiwww.cnki . net

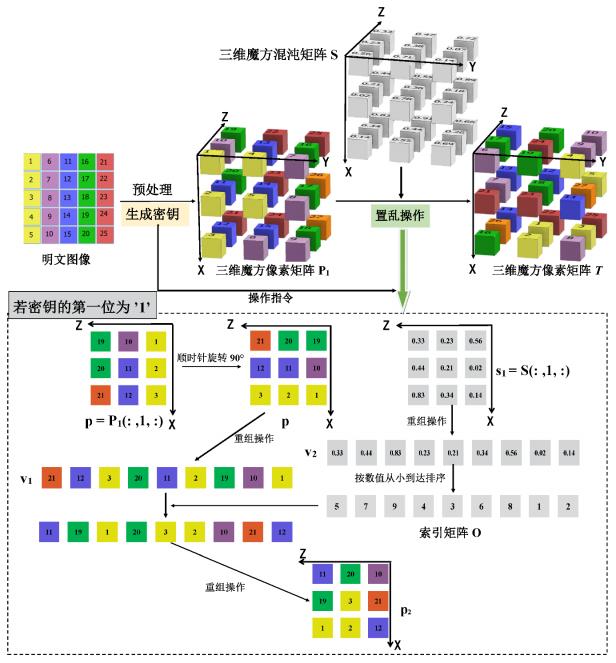


图 3-6 CMCT 置乱的演示

Fig. 3-6 Demonstration of CMCT permutation

明文图像经过三轮置乱、扩散操作后可得到一个尺寸为  的三维魔方像素 矩阵，需将其转换成二维平面图像，具体过程如下：首先计算m  vb,xb,xb ，若 *m* 为整数，其保持不变；否则m  floor(m)  ~~I~~  1 ，即先向下取整后再增加 1。然后， 构建一 个尺寸为mx m 的二维空矩阵，随后将上述三维魔方像素矩阵的所有元素依次放至构建 的二维空矩阵中，并用数量为m 2  bi3 的随机整数填充至二维空矩阵中的空余部分，且随 机整数的选取范围为 [0,255 。最终所得的二维像素矩阵即为密文图像 *C*。

24

中国知网 https:iiwww.cnki . net

**3.2.2 算法的解密过程**

本章所设计算法的解密过程与加密过程之间互为可逆过程。其解密过程步骤如下： 步骤 1：读取密文图像 *C*，由上述加密过程可知，密文图像 *C* 的大小为mx m 。

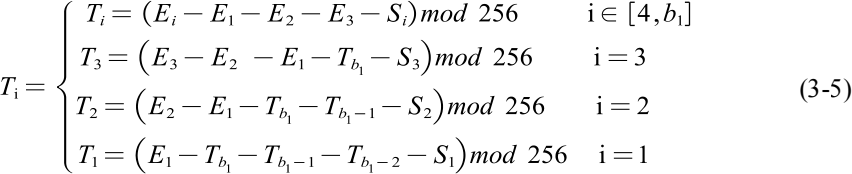
步骤 2：读取密钥，由密钥第一部分可获取二进制数的总数量为3xb, ；由密钥第二 部分可获取无平衡点混沌系统的参数；由密钥第三部分可获取明文图像的尺寸为M  N 。

步骤 3 ：选取密文图像c 中的前bi3个像素， 剩余像素可直接舍弃，并将所选取像素 转换成一个大小为b1xb1xb, 的三维魔方像素矩阵。

步骤 4：与加密过程相同，利用密钥使得无平衡点混沌系统生成三维魔方混沌矩阵。

步骤 5 ：先利用三维魔方混沌矩阵对三维魔方像素矩阵进行反扩散操作得到新的三 维魔方像素矩阵，再利用密钥第一部分与三维魔方混沌矩阵对反扩散操作所得的三维魔 方像素矩阵进行反置乱操作，并且反扩散-反置乱操作进行三轮，最终获得一个大小为  的三维魔方像素矩阵，其中，反置乱操作未置乱操作的逆过程，而反扩散操 作的具体过程如式(3-5)所示。

步骤 6：从步骤 5 所得的三维魔方像素矩阵选取前M  N 个像素，剩余像素可直接 舍弃，并将所选取像素转换成尺寸为M  N 的二维像素矩阵，即为解密图像。



**3.3** **算法仿真分析**

本节对提出的图像加密算法（CMCT-IEA）进行仿真测试。使用 CMCT-IEA 对不同 种类的图像进行加、解密测试，并且所有的测试图像来自南加州大学图像数据库(USC- SIPI)、布朗大学大型二值图像数据库。另外，本节还分析了 CMCT-IEA 的加密效率。

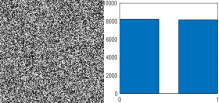
**3.3.1 仿真结果**

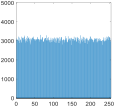
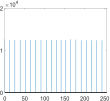
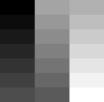
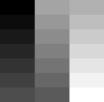
图像加密算法应能对任意类型的数字图像进行加密，并且仅在密钥完全正确的情况 下才能实现相应的解密操作。图 3-7 为 CMCT-IEA 对不同类型图像的加密仿真结果，其 中，第一行为二进制图像的测试结果，第二、三行为灰度图的测试结果， 第四行为 RGB 彩色图像的测试结果。对比图 3-7 中的(a)列与(c)列可知，明文图像经 CMCT-IEA 加密后 产生了巨大的变化。此外，由(b)列与(d)列可以看出，各明文图像的像素分布状况都具备 一定的特点，可根据这些像素分布特点对各明文图像进行区分。而各密文图像的像素分 布状况十分均匀，因此无法根据像素分布状况做出任何判断。另外， 根据(e)列可知，图

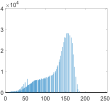
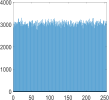
25

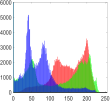
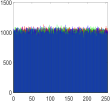
中国知网 https:iiwww.cnki . net

像加密算法可根据相应密钥能够将密文图像完全复原为明文图像。









(a)明文图像 (b)(a)的直方图 (c)密文图像 (d)(c)的直方图 (e)解密结果 图 3-7 CMCT-IEA 对不同类型图像的加密仿真结果

Fig. 3-7 Simulation results of CMCT-IEA encryption for different types of images

**3.3.2 效率分析**

对于本章所提出的图像加密算法，其加密过程中的耗时部分主要包括三个方面：混 沌序列的生成、排列和扩散。假设一个普通图像的大小为  ，第一部分主要是生成 4 组长度为 的混沌序列    ，对应的时间复杂度为  ；第

二部分主要为对三维空间中的像素平面进行置乱以及对各平面中的像素进行置乱操作， 时间复杂度为  最后一部分为计算数量为  像素值，对应的 时间复杂度为  。由于加密算法中包含三轮置乱、扩散操作，因此算法加密该图

像总的时间复杂度为  。另外，在 Matlab

2018b 平台上使用该算法对不同尺寸的图像进行加密，使用的硬件平台为 Intel(R) Core(TM) i5-1130H CPU @ 3.10 GHz, 16GB 内存, Windows10 操作系统。表 3-2 列出了 CMCT-IEA 加密尺寸为 、 、 、 的灰度图像的加密

时间。

表 3-2 CMCT-IEA 对不同尺寸图像的加密时间

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 图像尺寸 | 128  128 | 256  256 | 512  512 | 1024  1024 |
| 加密时间（秒） | 0.086 | 0.205 | 0.768 | 2.679 |

**3.4** **算法的安全性能分析**

本节对 CMCT-IEA 的加密安全性进行了测试分析，具体包括统计特性分析、密钥分 析、差分攻击分析以及鲁棒性分析等方面。

**3.4.1 统计特性分析**

统计分析的主要工作包括直方图分析、相关系数分析以及信息熵等方面。

（1）直方图分析

直方图常用于描述图像像素值的分布状况。一般来说，密文图像各像素值之间的出 现频次十分接近，难以从中得到有效的统计信息。从图 3-7 可以看出，密文图像的直方 图（图 3-7 (d)）比初始图像直方图（图 3-7 (b)）更平坦、均匀。此外， 本节还使用了卡 方测试来检验密文图像直方图的均匀程度，卡方计算方式具体如下：

 (3-6)

其中，on 与en 原始图像和密文图像的像素出现频率，当测试图像为灰度图像时 *n* = 256， 给定显著性水平值a  0 . 05 ，此时 X 2 的理想值为 293.2478。表 3-3 展示了从 USC-SIPI 图像数据库中选取的明文图像与其对应密文图像的卡方值计算结果。

由表 3-3 中测试结果可知，密文图像的卡方值远比明文图像的卡方值更接近理想值， 因此密文图像的像素分布更均匀。

表 3-3 CMCT-IEA 的卡方测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| 图像 |  | | 2 |
| 明文图像 | 密文图像 | |
| harrierocc3 (128  128) | 2.8601×106 | 224.7914 | |
| House (256  256) | 3.0085×105 | 260.9469 | |
| 7.1.09.tiff (256  256) | 9.5795×105 | 260.2852 | |
| Lena (512  512) | 3.9869×104 | 258.2708 | |
| gray21.512 (512  512) | 2.9336×106 | 263.4258 | |

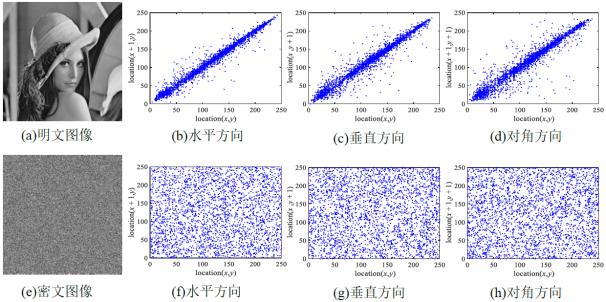


图 3-8 “Lena”图像与密文图像的相关性

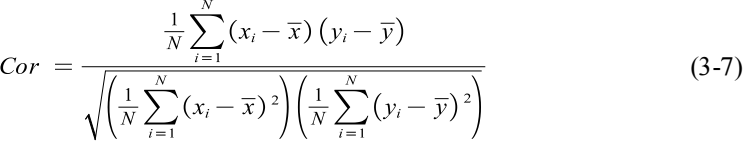
Fig. 3-8 Correlation of original and encrypted “Lena”

表 3-4 不同图像的像关系数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 图像 | | 水平方向 | 垂直方向 | 对角方向 |
| Lena  (256  256) | 明文 | 0.9541 | 0.9249 | 0.9113 |
| 密文 | -0.0025 | 0.0020 | -0.0003 |
| Lena  (512  512) | 明文 | 0.9864 | 0.9679 | 0.9542 |
| 密文 | 0.0028 | -0.0034 | -0.0041 |
| House  (256  256) | 明文 | 0.9536 | 0.9787 | 0.9421 |
| 密文 | -0.0070 | -0.0044 | 0.0009 |
| Peppers  (512  512) | 明文 | 0.9509 | 0.9764 | 0.9337 |
| 密文 | 0.0013 | 0.0039 | 0.0037 |

（2）相邻像素相关性分析

数字图像所具备的最大特征之一便是信息冗余，这使得图像的相邻像素通常拥有较 高的关联程度，但这对于图像的信息安全而言显然是一个极大的弊端。因此， 图像加密 算法应能够有效降低相邻像素之间的相关性。相邻像素之间的相关性包括水平、垂直和 对角方向相邻像素相关性，其公式定义如下：



其中，*x* 与*y* 互为相邻像素，  与 分别对为 *x* 与*y* 的平均值，*N* 为选取的像素对数量。 并且加密后的密文图像的相关系数值应接近于 0 。选取“Lena”图像作为明文图像并利 用 CMCT-IEA 对其加密，再从加密前后的图像中分别随机选取 3000 对像素点作为测试 输入。图 3-8 展示了加密前后图像相邻像素在不同方向的关联程度。其中， 明文图像加 密前的相邻像素之间具有较强的关联性，而加密后的相邻像素之间无明显关联。表 3-4 展示了多个图像的测试结果。另外， 表 3-5 中给出了CMCT-IEA 与其他算法加密尺寸为 256  256 的“Lena”图的相关系数测试对比结果，显然，CMCT-IEA 加密所得的相关系 数更接近 0。以上结果均表明，本章所提出的 CMCT-IEA 能够有效抵御统计攻击。

表 3-5 相关系数对比结果

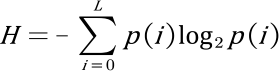
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lena 图像 | 加密算法 | 水平 | 垂直 | 对角 |
| 明文 | 0.9541 | 0.9249 | 0.9113 |
| 密文 | CMCT-IEA | -0.0025 | 0.0020 | -0.0003 |
| 文献[6] | 0.0025 | 0.0013 | 0.0013 |
| 文献[7] | -0.0017 | -0.0084 | -0.0019 |
| 文献[64] | 0.0230 | 0.0280 | 0.0230 |

表 3-6 CMCT-IEA 的信息熵测试结果以及与其他算法的比较

|  |  |  |
| --- | --- | --- |
| 图像 | 明文 | 密文 |
| Cameraman (256  256) | 7.0097 | 7.9973 |
| 5.1.09.tiff (256  256) | 6.7093 | 7.9976 |
| 5.1.13.tiff (256  256) | 1.5483 | 7.9972 |
| 7.1.03.tiff (512  512) | 5.4957 | 7.9993 |
| Lena (512  512) | 7.4451 | 7.9994 |
| Lena (256  256) | 7.4429 | 7.9976 |
| 文献[7] | - | 7.9975 |
| 文献[19] | 3.6347 | 7.9976 |
| 文献[48] | - | 7.9975 |

（3）信息熵

信息熵反映了图像信息的不确定性。通常，密文图像中所包含的信息应该是随机的， 其对应的熵值应趋于理论值。计算信息熵的公式可表示为：

 (3-8)

其中，*L* 为图像的像素级数，P(i)是像素数值为i 的像素出现概率。例如，灰度图像的 素级数L  255 ，并且理论熵值为 8 。表 3-6 展示了几种不同内容的灰度图像的对应熵 值，并与现有的几种算法进行了比较。结果表明，CMCT-IEA 算法优于其他几种算法。

**3.4.2 密钥安全分析**

密钥安全性是评估密码系统安全性能的重要指标，其具体评估内容包括密钥空间与 密钥敏感性。本节将从以上两方面对 CMCT-IEA 中密钥安全性进行评估分析。

（1）密钥空间分析

为了抵御暴力穷举攻击，图像加密算法的密钥空间应大于2ioo 。对于 CMCT-IEA ， 其密钥主要由三个部分组成。第一部分：根据预处理所得的结果b, ，随机生成长度为 3  bi 的二进制数组ki 。第二部分： 无平衡点混沌系统的初始参数。第三部分： 明文图像 的行数与列数。该密钥生成方法增强了密钥与明文图像和算法之间的相关性。当原始图 像的尺寸不同时，生成的密钥也不同，这种动态密钥提高了算法的加密性能。由于密钥 与明文图像的尺寸具有较强的相关性，因此其密钥空间也由明文图像的尺寸所决定。若 待加密图像的尺寸为64  64 ，经预处理操作可得到对应的b,  16 ，则密钥第一部分为一 个数量为 48 位的二进制数组，混沌系统参数 d, k 的步长为10 - 14 ，因此密钥空间为 248x1014x2x2141 。根据密钥的结构特征，密钥空间的大小与明文图像的尺寸大小呈正 相关。而常见的数字图像的尺寸均大于64  64 。因此， CMCT-IEA 在加密常见的数字图 像所提供的密钥空间至少为214i ，这表明 CMCT-IEA 具备较强的抵御暴力穷举攻击能力。

（2）密钥敏感性分析

图像加密算法对密钥的变化也应该当极其敏感，即使密钥产生很小的变化，但最终 加解密的结果之间也应是天差地别的。在本节中，我们以USC-SIPI图像数据集中的图 “5.1.09.tiff”为例进行密钥敏感性测试。对于初始密钥ko ，将ko 的第一位二进制数变 为相反值得到密钥ki ，再令KO 中混沌参数K  55 . 9999 得到密钥K2 。其中K,  {AEF71

DBFF6307D3FFF86FFBDDBF8B7EFED7EBF773; 4 , 16 , 10 , 16 , 56; 512 , 512};K  {BE F71DBFF6307D3FFF86FFBDDBF8B7EFED7EBF773;4 , 16 , 10 , 16 , 56; 512 , 512};K2  {BEF71DBFF6307D3FFF86FFBDDBF8B7EFED7EBF773; 4 , 16 , 10 , 16 , 55 . 9999; 512 ,

512} ；然后，进行加密敏感性测试：分别将K, 与ki作为加密密钥，得到密文图像CO与

ci 分别如图3-9(b)与(c)所示，并且它们之间的差值Co  cil 如图3-9中(d)所示。解密敏感 性测试：分别使用密钥KO 、K 与K2 对CO进行解密，所得的解密结果D, 、Di 与D2 分别 如图3-9(e)、(f)、(g)所示，并且Di 与D2 之间的差值 D2  Di 如图3-9(h)所示。由图3-9(d) 可知，在加密过程中，即使密钥发生了极小的改变，所得的加密结果之间也大相径庭， 这表明CMCT-IEA的加密过程对密钥极其敏感。由图3-9(e)、(f)、(g)可知，在解密过程中 只有在密钥完全正确的情况下才能完成解密，另外，由图3-9(h)可知，密钥之间的微小差

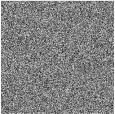
30

中国知网 https:iiwww.cnki . net

异会导致解密的结果大不相同，这表明CMCT-IEA的解密过程对密钥也十分敏感。综上， CMCT-IEA具备较好的密钥敏感性。



(a)明文图像 (b)密文图像 *C*0 (c)密文图像 *C*1 (d) | *C*0 - *C*1 |结果



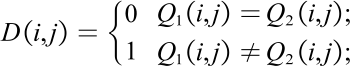
(e)解密结果 (f)解密结果 (g)解密结果 (h) | *D*1 – *D*2 |结果

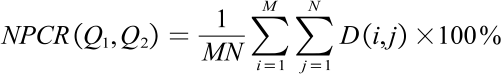
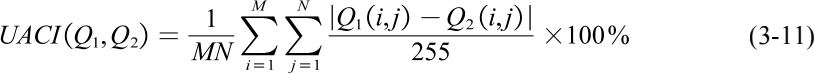
图 3-9 密钥敏感性分析

Fig. 3-9 Key sensitivity analysis

**3.4.3 差分攻击分析**

差分攻击是一种选择明文攻击方法，通过分析具备特定差异的明文在通过加密前后 的变化规律来攻击密码系统，具体表现为通过统计图像相同位置的像素点之间位置变化 率(NPCR)与像素数值的变化强度(UAcn)来获取加密过程中像素的变化状况。为测试 CMCT-IEA的抗差分攻击能力，进行以下测试：利用CMCT-IEA对明文图像pi 加密，加 密结果为Qi ；改变pi 中任意一个像素点的值后得到P2 ，并对P2 加密得到Q2 ；其中，上 述两次加密过程中，除pi 与P2 之间存在微小差异，其它条件均相同。针对以上测试结果 Qi 与Q2 ，利用式(3-9) ~ (3-11)计算出相应的*NPCR*与*UACI*值。

 (3-9)

 (3-10) 

其中，*M*、*N* 为被测试图像的尺寸 ，*NPCR* 与 *UACI* 的理论值分别为 99 . 6094% 与 33 . 4635% 。为评估 CMCT-IEA 的抗差分攻击能力，选取图像“5.1.09.tiff”，“Lena ”， “Tank ”为测试对象，表 3-7 展示了以上测试结果以及其他算法加密图像“Lena ”的 NPCR 与UAcr测试结果。由表 3-7 可知，CMCT-IEA 对不同图像的测试结果都较为良

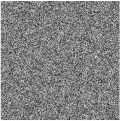
31

中国知网 https:iiwww.cnki . net

好，并且相较于其他加密算法，其平均结果也更接近理论值，这表明CMCT-IEA 能够有 效抵御差分攻击。

表 3-7 CMCT-IEA 的 NPCR 和 UACI 测试结果以及与其他算法的比较

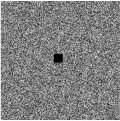
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Lena | Tank | 5.1.09.tiff | 文献[7] | 文献[19] | 文献[48] |
| NPCR | 99.6039% | 99.6082% | 99.6053% | 99.6180% | 99.6017% | 99.6017% |
| UACI | 33.4617% | 33.4489% | 33.4750% | 33.4960% | 33.4619% | 33.4619% |



(a)密文图像



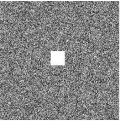
(d) (a)的解密结果



(b)将(a)裁剪 0.5%



(e) (b)的解密结果



(c)将(a)裁剪%1.5%



(f) (c)的解密结果

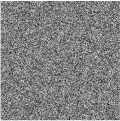
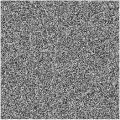
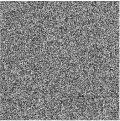
图 3-10 抵御裁剪攻击测试

Fig. 3-10 Resistance to cropping attack analysis.

**3.4.4 鲁棒性分析**

密文图像在传输过程中很容易被攻击者截获。当攻击者无法破解密文图像时，通常 采用通信干扰作为攻击手段，阻止接收方获取完整的信息。其中， 裁剪攻击和噪声攻击 是常用的攻击方法。本节对 CMCT-IEA 进行了不同程度的裁剪攻击和不同类型的噪声 攻击试验。图 3-10 为 CMCT-IEA 抗裁剪攻击分析，其中 ，图 3-10(a)为密文图像，分别

将图3-10(a)裁剪0 . 5% 与1 . 5% 得到图3-10(b)与(c)，随后分别对以上密文图像进行解密， 所得的对应结果为图 3-10(d)-(f) 。图 3-11 为 CMCT-IEA 抗噪声攻击分析，其中 ，图 3- 10(a)为密文图像，分别对图 3-10(a)加入1 . 5% 的椒盐噪声、0 . 3% 的斑点噪声以及 5%的 泊松噪声得到图 3-10(b)-(d)，随后对以上密文图像进行解密，所得的解密结果对应为图 3-10(d)-(g)。由以上测试结果可以看出，当密文图像遭受不同类型的噪声和不同程度的 裁剪攻击时，CMCT-IEA 的解密过程仍然可以恢复明文图像。虽然恢复的图像仍存在噪 声，但它们仍然可以提供大部分的信息，这表明CMCT-IEA 能够有效抵抗裁剪攻击和噪 声攻击。



(a) 密文图像 (b) 1.5%椒盐噪声 (c) 0.3%斑点噪声 (d) 5%泊松噪声



(e) (a)的解密结果 (f) (b)的解密结果 (g) (c)的解密结果 (h) (d)的解密结果

图 3-11 抵御操作攻击测试

Fig. 3-11 Resistance to noise attack analysis

**3.5** **本章小结**

本章提出了一种基于无平衡点混沌系统的混沌魔方变换图像加密算法(CMCT-IEA)。 利用一种具备更复杂混沌行为的无平衡点混沌系统生成的混沌序列参与CMCT-IEA的置 乱和扩散过程。其中， 该算法的置乱操作可以在三维空间中打乱图像像素，而扩散操作 能够在三维空间中扩散明文图像微小的像素变化。该算法可根据明文图像生成一种动态 密钥，并且具备较大的密钥空间，可以抵抗暴力攻击。统计分析结果表明，由CMCT-IEA 加密所得的密文图像具备较高的信息熵值以及极低的相邻像素相关性。另外，安全测试 结果也证明了其具有优异的安全性能。

33

中国知网 https:iiwww.cnki . net

**第四章** **基于** **2D-Price 混沌映射的同步置乱-扩散图像加密算法**

针对一些对图像加密效率要求较高的应用场合，本章设计了一种基于 2D-Price 混沌 映射的索引同步置乱-扩散图像加密算法（ISPD-IEA）。首先，基于经典的 Price 函数提 出了一种新的 2D-Price 映射并对其安全性能进行分析，分析结果表明该映射能够在一个 极大的参数范围内表现出优异的超混沌特性。在此基础上， 本章还设计了一种基于索引 的同步置乱-扩散机制，最终得到了 ISPD-IEA 。该算法将传统的置乱、扩散过程结合为 一个整体，这使得其能够在改变图像像素位置的同时还能图像像素的微小变化扩散至全 局。明文图像经两轮加密操作后可快速变为肉眼无法识别的噪点图像。与其他加密算法 相比，ISPD-IEA 的结构具有更好的完整性，有利于抵御攻击者的差分分析攻击。实验仿 真与测试分析结果表明，ISPD-IEA 具有良好的安全性和极高的加密效率。

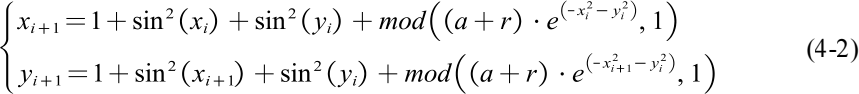
**4.1 2D-Price 混沌映射的设计与分析**

Price 映射的设计灵感源自广泛应用于优化函数基准的 Price 函数。1977 年，W. L. Price 首次提出 Price 函数用于测试优化算法，Price 函数可由下式表示[63]：

f(x,x2)  1  ~~I~~  Sin2 (x)  ~~I~~  Sin2 (x2)  0 . le 2 (4-1)

(  xi2 x2)

Price 函数具备对称且多模态的特性，因此其拥有多个最优值。它的全局最小值为 f(x  o , x2  o)  o . 9 ，并且其所有的函数值在[0.90 , 2.99] 中变化。事实上， 式(4-1) 中的sin2 (x)  ~~I~~  Sin2 (x2)部分是 Price 函数能够具备以上特性的重要原因。鉴于其它经典 混沌映射（Tent 映射[26] 、Logistic 映射[39] 、Sine 映射[54]）的改进工作，本章对 Price 函 数也进行了改进，最终提出了一个 2D-Price 混沌映射。所提出的 2D-Price 混沌映射如下 式所示：



其中，a ，r 是控制参数，当a  10" 且r  (0,) 时，2D-Price 混沌映射处于超混沌状态。 xi ，yi 为状态变量，xi  i 与yi  1 分别为它们的下一次迭代值。令状态变量xi 与yi 的初始 值为 0.5,初始参数a  10" ，系统在参数r  [0, 10] 的分岔图如图 4-1 所示。图 4-2 展示 了 2D-Price 混沌映射的状态变量初始值xo  0 . 5 、y 0 . 5 ，初始参数a  10" 且r  5 时所对应的混沌运动轨迹。由图 4-1 与图 4-2 可知，本章所提出的2D-Price 混沌映射具 备较为复杂的非线性特征。此外，本节还分析了 2D-Price 混沌映射的 Lyapunov 指数， 所对应的初始条件为：状态变量xi 与yi 均为 0.5 ，参数a  109 ，r  [0, 10 。由图 4-3

34

中国知网 https:iiwww.cnki . net

可知，本章所提出的 2D-Price 混沌映射具有两个较大的正的 Lyapunov 指数，这表明该 系统具备优异的混沌特性。

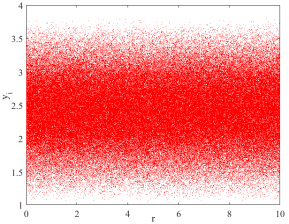


图 4-1 2D-Price 映射分岔图

Fig. 4-1 The bifurcation diagram of 2D-Price map

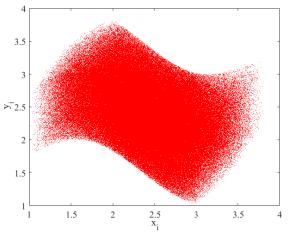


图 4-2 2D-Price 映射的混沌吸引子图

Fig. 4-2 The chaotic attractor diagram of 2D-Price map

14

12

1 0

8

6

4

2

|  |  |  |
| --- | --- | --- |
|  | | |
|  | |  | | --- | | LE2 | |  |
|  | | |
|  | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2 | 3 | 4 | 5 r |  | 7 | 8 |  |

图 4-3 2D-Price 映射的 Lyapunov 指数图

Fig. 4-3 The Lyapunov exponent diagram of 2D-Price map

35

中国知网 https:iiwww.cnki . net

混沌系统生成的混沌序列应当具备良好的随机性，本节采用 NIST SP800-22 测试了 其生成的混沌序列的随机性。由表 4-1 可知，2D-Price 映射生成的混沌序列具备较好的 随机性，因此其适用于设计图像加密算法。

表 4-1 2D-Price 混沌映射生成的二进制序列的 NIST SP800-22 测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| 子测试 | | P 值 (≥0.01) | 结果 |
| 单比特频率 | | 0.7703 | 通过 |
| 频率块 | | 0.5553 | 通过 |
| 游程 | | 0.1802 | 通过 |
| 最长游程 | | 0.7394 | 通过 |
| 二进制矩阵秩 | | 0.0336 | 通过 |
| 离散傅氏变换 | | 0.5814 | 通过 |
| 非重叠模板匹配 | | 0.1159 | 通过 |
| 重叠模板匹配 | | 0.4351 | 通过 |
| 通用统计 | | 0.6526 | 通过 |
| 线性复杂度 | | 0.6085 | 通过 |
| 随机游动 | | 0.6739 | 通过 |
| 随机游动状态频数 | | 0.4134 | 通过 |
| 近似熵 | | 0.5876 | 通过 |
| 序列测试 | P 值 1 | 0.0513 | 通过 |
| P 值 2 | 0.0589 | 通过 |
| 累加和 | 正向 | 0.6755 | 通过 |
| 反向 | 1.0000 | 通过 |

**4.2** **ISPD 图像加密算法**

为了寻求一种安全高效的图像加密策略，本节利用 2D-Price 混沌映射设计一种基于 索引的同步排列-扩散图像加密算法（ISPD-IEA），图 4-4 展示了其具体加密流程。首先， 利用密钥生成 2D-Price 混沌映射的初始控制参数 *r* ，进而获得相应的混沌序列。然后， 对混沌序列和明文图像进行加和、取模运算，得到随机像素矩阵。最后，利用混沌矩阵 对像素矩阵进行两轮 ISP-DTM 操作，得到密文图像。

|  |
| --- |
| 密钥 |

|  |
| --- |
| 混沌系统参数 |

|  |
| --- |
| 明文图像 |

|  |
| --- |
| 2D-Price映射 |



加和、取模

|  |
| --- |
| 混沌序列 |

|  |
| --- |
| 随机像素矩阵 |

|  |
| --- |
| 密文图像 |

ISP-DTM

两 轮

图 4-4 ISPD-IEA 结构图

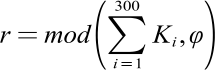
Fig. 4-4 The structure of ISPD-IEA

（1）混沌序列的生成

首先，将密钥k 设置成长度为 300 位的二进制序列，因此其密钥空间为23oo 。然后， 设置 2D-Price 混沌映射初始条件xo 、yo 、( 、*r*。其中，xo  0 . 5 , yo  0 . 5 ，a  1o9 ， *r* 的取值由密钥k 决定，具体计算方式如式(4-3)与(4.4)所示。最后，2D-Price 混沌映射 可生成两组混沌序列。

100 200 300



 (4-4)

（2）随机像素矩阵的生成

由图 4-4 可知，2D-Price 混沌映射生成的混沌序列与明文像素矩阵经加和、取模操 作得到一个随机像素矩阵。具体过程为： 假设明文图像 *O* 的尺寸为M  N 。首先， 利用 2D-Price 混沌映射生成尺寸同样为M  N 的混沌矩阵 *S*。然后， 对混沌矩阵 *S* 与明文图 像之间进行加和、取模操作，得到随机像素矩阵 *P*。最终， 随机像素矩阵 *P* 可由式(4-5) 表示。

P  mod(mod(floor(s · 232) , 256)  ~~1~~  0, 256)

(4-5)

37

中国知网 https:iiwww.cnki . net

（3）ISP-DTM 的描述

数字图像相邻像素间的高相关性使其存在较高的信息冗余，这可能为攻击者的破译 工作提供便利。因此，在对数字图像进行加密时，降低图像像素间的关联程度是必要的。 大多数图像加密算法在对加密图像时主要采用两种策略：置乱与扩散。其中， 前者主要 用于打乱像素排列顺序，而后者则用于改变像素强度。另外，为获得优异的安全性能， 这些图像加密算法往往采用了多轮的置乱-扩散结构，这可能会为其衍生出一些负面影 响，如降低加密效率、加密时会产生的中间信息使得算法容易被攻击者破解等。为解决 以上所存在的问题， 本节设计了一种基于索引的同步排列-扩散图像加密转换机制 （ISPD-DTM），它将置乱与扩散的特性进行耦合，使其能够在改变像素位置的同时，也 能将任意像素的细微变化影响至全局。ISPD-DTM 可以有效避免多轮加密过程的负面影 响，具有更好的加密效率和安全性能。

假设明文图像 *O* 与混沌矩阵 *S* 经加和、取模操作后得到随机像素矩阵 *P*，并且它们 的尺寸均为M  N 。ISP-DTM 加密过程的详细描述如下：

步骤 1 ：对混沌矩阵s 的第 1 行混沌值进行升序排列，得到索引向量 *Index*1，并且 该索引向量的尺寸为1 × N；

步骤 2：根据 *Index*1 ，从随机像素矩阵 *P* 的第 1 行像素中选取相应的像素作为密文 矩阵c 的第 1 行像素，即c(1 ,j)  P(1 , Inder I (1 ,j)) (j  1 N) ；

步骤 3 ：将混沌矩阵 *S* 的第i(i  2)行像素分别与密文矩阵c 的第i  1(i  2)行混 沌值相乘进而获得 1 个一维数值矩阵，然后对其所有的数值进行升序排列，得到索引向 量 *Index*2；

步骤 4：根据 *Index*2，从随机像素矩阵 *P* 的第i(i  2)行像素中选取相应像素作为密 文矩阵 *C* 的第i(i  2)行像素，即c(i,j)  P(i  1 , Index2(1 ,j)) (i  2 ,j  1 ~N)；

步骤 5：对每一行进行步骤3 ~ 4 中的操作，并且i  3 M ，最终得到密文矩阵 *C*；

步骤 6 ：将密文矩阵C 顺时针旋转90- 得到一个新的像素矩阵，并在该像素矩阵上 重复步骤1 ~ 5 得到 ISPD- DTM 的加密结果。

图 4-5 给出了ISPD-DTM 加密过程的示例。其中，*O* 为明文图像，*S* 为混沌矩阵， *O* 与 *S* 进行加和、取模操作后得到的随机像素矩阵*P*。具体加密过程如下：

将混沌矩阵 S 的第 1 行混沌序列按数值从小到大进行排序， 得到索引 向量 *Index1*={3,1,2,4,5}，然后，根据Index l ，从随机像素矩阵 *P* 的第 1 行像素中选取相应的

像素作为密文矩阵 C 的第 1 行像素， 即 ca.n  P(i · 3 ， C( ,2)  P(i · 1) ， C · 3  P( · 2) ， C(i · 4  P(i · 4 ，C(i · 5  P(i · 5 ；

图中由“ S(2 , :)  C(1 , :) ”得到索引向量*Index*2 的过程如上述步骤 3 所描述，然 后，再根据 *Index*2，从随机像素矩阵 *P* 的第 2 行像素中选取相应的像素作为密文矩阵 *C*

的第 2 行像素，即C2.1  P2 · n ，C(2, 2)  P(2, 3 ，C(2. 3)  P(2 · 5) ，C2 · 4)  P2 · 4 ，C2 · 5)  P2, 2) ；

38

中国知网 https:iiwww.cnki . net

根据索引向量 *Index*3，从随机像素矩阵 *P* 的第 3 行像素中选取相应的像素作为密文

矩阵 *C* 的第 3 行像素，即C(3 · n  P(3 , 2) ，C(3 , 2  P(3 · i ，C(3 · 3  P(3 , 3 ，C(3 , 4  P(3 , 4) ， C3 · 5  P3 · 5) ；

根据索引向量 *Index*4，从随机像素矩阵 *P* 的第 4 行像素中选取相应的像素作为密文

矩阵 *C* 的第 4 行像素，即C(4 · i  P(4 · 1 ，C(4, 2  P(4, 4 ，C(4, 3  P(4 · 3 ，C(4 · 4)  P(4 · 5 ， C(4 · 5  P(4 , 2) ；

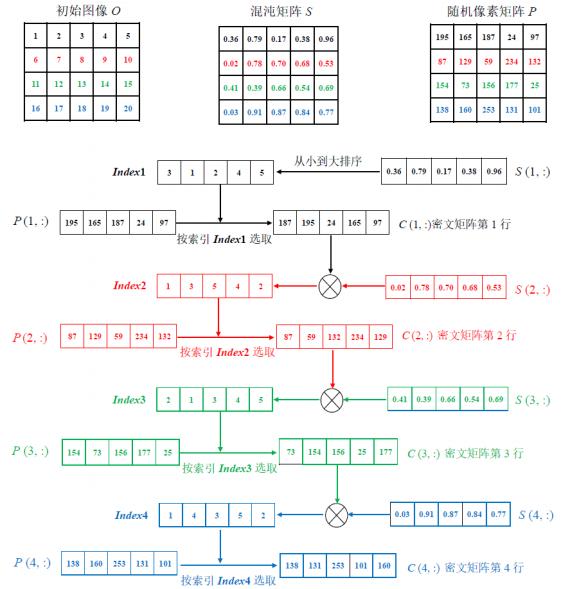


图 4-5 ISPD-DTM 加密过程的示例

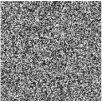
Fig. 4-5 An example of the ISPD-DTM encryption process

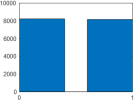
ISPD-DTM 的优点是，当一行/列像素被加密时，它产生的变化将被传递至下一行/ 列，这使得其在打乱像素位置的同时还能扩散像素的变化。

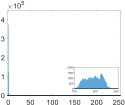
39

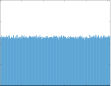
中国知网 https:iiwww.cnki . net

**4.3** **算法仿真分析**

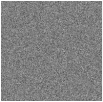
本节对提出的ISPD-IEA 进行加密仿真实验，同时还分析了它的加密效率。

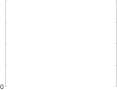
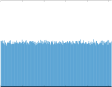
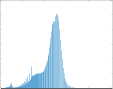






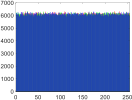
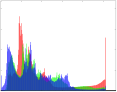
250



12000 10000

0 50 100 150 200 250

200 250

104

4

3

2

1

0 50 100 150 200 250

(a)明文图像

Fig. 4-6

(b) (a)的直方图 (c) 密文图像 (d) (c)的直方图 (e) 解密结果

图 4-6 ISPD-IEA 对不同类型图像的加密仿真结果

Simulation results of ISPD-IEA encryption for different types of images

**4.3.1 仿真结果**

本节使用 ISPD-IEA 对不同类型的图像进行加密仿真，并得到相应的实验结果。其 中，实验中所使用的测试图例选自南加州大学图像数据库、布朗大学大型二值图像数据 库和日常摄影作品。图 4-6 显示了二进制、灰色和彩色图像的加密结果。从图 4-6 中的 (a)与(c)可以看出，加密前后的图像之间几乎无任何相似性。在解密过程中，使用与加密 过程中所使用的密钥可成功实现解密工作，4-6(e)展示了对应的解密结果。

**4.3.2 效率分析**

本章所提出的 ISPD-IEA 具备较低的时间复杂度，主要有以下原因：（1）算法中采 用了二维离散混沌系统，计算花销较小；（2）ISP-DTM 加密过程中能够同时达到置乱与 扩散的效果，工作效率高；（3）从算法的全局结构来看，ISPD-IEA 在具备高安全性的前 提下，仅包含两轮 ISP-DTM 加密操作。

40

中国知网 https:iiwww.cnki . net

ISPD-IEA 的耗时部分主要包括两部分：获取混沌序列，ISP-DTM 的加密过程。假 设所加密的明文图像尺寸为M  N ，前者需要生成两组长度为M  N 的混沌序列，对应 的计算复杂度为O(2  M  N) ；而 ISP-DTM 改变图像中所有像素的位置和像素值，对 应的计算复杂度为O(4  M  N  ~~I~~  MlogN  ~~I~~  NlogM) ，并且加密过程中包含两轮 ISP- DTM。因此，ISPD-IEA 总的计算复杂度为O(10  M  N  2MlogN  ~~I~~  2NlogM)。另外， 本节还测试了 ISPD-IEA 的加密速度，测试环境如下：Matlab 2018b 、windows 10 操 作系统、3.10 GHz CPU 、16 GB 内存等。使用 ISPD-IEA 对不同尺寸的灰度图像加密， 测试结果如表 4-2 所示。

表 4-2 ISPD-IEA 加密不同尺寸的图像所需时间

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 图像尺寸 | 128  128 | 256  256 | 512  512 | 1024  1024 |
| 加密时间（秒） | 0.035 | 0.093 | 0.302 | 1.143 |

表 4-3 ISPD-IEA 加密不同图像的卡方测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| 图像 |  | | 2 |
| 明文图像 | 密文图像 | |
| Lena (256  256) | 39869 | 242.3125 | |
| 5.1.09.tiff (256  256) | 300850 | 251.1094 | |
| Cameraman (512  512) | 418530 | 229.4180 | |
| Tank (512  512) | 957950 | 241.9043 | |

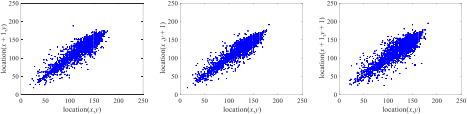
**4.4** **算法的安全性能分析**

（1）直方图分析

直方图是一种描述图像中像素数量分布的方法，可以通过计算图像中所有像素级别 的数量来获得。直方图的计算结果仅由图像的像素组成所决定，攻击者可通过对比图像 在加密前后的直方图来确定目标图像信息。为了防御这种攻击， 可靠的图像加密算法应 该能够加密任意图像，并且各加密结果的直方图应具有较高的相似的。由图 4-6(b)可知， 明文图像的像素分布状况各具特色，而密文图像的像素（图 4-6(d)）分布状况均十分均 匀且相似度极高。

此外，本节还利用卡方测试加密前后图像的直方图进行了定量分析。根据式(3-6)， 分别计算图 4-6 中各明文图像与对应密文图像的卡方值，计算结果如表 4-3 所示。由表 4-3 可知，ISPD-IEA 加密所得的密文图像的卡方值远比对应明文图像的卡方值接近于理 论值。



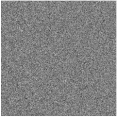


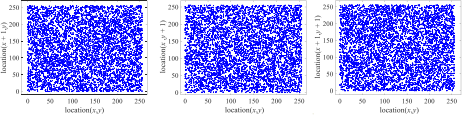
(d) 对角方向

(b) 水平方向

(c) 垂直方向

(a) 明文图像





(h) 对角方向

(g) 垂直方向

(f) 水平方向

(e) 密文图像

图 4-7 “Tank”与其密文图像的相邻像素相关性

Fig. 4-7 Adjacent pixel correlation of plain and encrypted “Tank” 表 4-4 ISPD-IEA 对不同灰度图像加密前后的相关系数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 图像 | | 水平方向 | 垂直方向 | 对角方向 |
| Lena | 明文 | 0.9620 | 0.9246 | 0.9108 |
| 密文 | 0.0026 | 0.0036 | -0.0033 |
| 5.1.09.tiff | 明文 | 0.9536 | 0.9787 | 0.9421 |
| 密文 | -0.0070 | -0.0044 | 0.0009 |
| Cameraman | 明文 | 0.9509 | 0.9764 | 0.9337 |
| 密文 | 0.0013 | 0.0039 | 0.0037 |
| Tank | 明文 | 0.9295 | 0.9650 | 0.9157 |
| 密文 | 0.0014 | 0.0012 | -0.0012 |

（2）相邻像素相关性分析

令“Tank”图像作为明文图像并利用 ISPD-IEA 对其加密，再从加密前后的图像中 随机选取 3000 对相邻像素作为测试输入。图 4-7 展示了加密前后图像像素在各方向的 关联程度。不难看出，明文图像的相邻像素在各方向上呈线性分布，具有较强的关联性， 而密文图像的相邻像素几乎为随机分布状态，彼此之间无明显关联。另外， 相邻像素相 关性的强弱可通过相关系数对其进行定量评估，其中相关系数可根据式(3-7)计算获得。 表 4-4 展示了利用 ISPD-IEA 对 4 幅不同的图像加密前后的相关系数。显然，密文图像 的相关系数更接近理想值。这表明 ISPD-IEA 能够有效降低图像的相邻像素的关联程度。

（3）信息熵分析

密文图像的信息具有高度随机性时可使其难以被他人直接获取。测量图像随机性的

一种有效方法是信息熵，其计算方法如式(3-8)所示。本节选择了 4 幅不同灰度图像作为 测试对象，并且它们的尺寸为均为256  256 ，表 4-5 展示了它们加密前后的信息熵计 算结果。由表 4-5 可知，各明文图像的熵值均处于较低水平，而密文图像的熵值均大于 7.99，这表明密文图像中的信息高度随机。因此，ISPD-IEA 具备较好的加密性能。

表 4-5 ISPD-IEA 对不同图像的信息熵测试结果

|  |  |  |
| --- | --- | --- |
| 图像 | 明文 | 密文 |
| Lena (256  256) | 7.4429 | 7.9974 |
| 5.1.09.tiff (256  256) | 6.7093 | 7.9973 |
| Cameraman (512  512) | 7.0480 | 7.9993 |
| Tank (512  512) | 6.1898 | 7.9993 |

（4）密钥分析

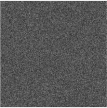
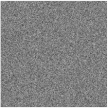
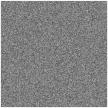
密钥的安性能取决于两个方面：密钥空间，密钥敏感性。对于图像加密算法， 为抵 御穷举暴力攻击，其密钥空间应大于2ioo ，并且其加密/解密的过程须对密钥的变化极端 敏感。

根据上文所述，ISPD-IEA 的密钥主要用于获取 2D-Price 混沌映射的初始参数r ，并 且r 可为任意实数，因此，ISPD-IEA 可具备无穷大的密钥空间。考虑到密钥对加密效率 的影响，本章讲密钥设置成一串长度为 300 比特的二进制序列值，并根据式(4-3)与式(4- 4)计算出初始参数r 。因此，ISPD-IEA 的密钥空间为23O0 ，远高于加密系统密钥空间的 要求，这表明 ISPD-IEA 能够低于暴力穷举攻击。

为了评估 ISPD-IEA 的密钥敏感性，本节进行了以下测试：首先，随机生成长度为 300 比特的二进制序列值作为初始密钥ko ，再分别改变密钥 ko 的第 10 位与第 100 位 二进制值，获得密钥ki ，K2 ，其中KO  F8E77EB2EF267B58DE77C3FC4DBB575B B7BDF73DCDB7997EFFA8FF5DF gB7356BBEEBgD7BB7B ;K1  F8A77EB2EF2 67B58DE77C3FC4DBB575BB7BDF73DCDB7F7997EFFA8FF5DFgB7356BBEEB 9D7BB; K2  F8E77EB2EF267B58DE77C3FC5FBB575BB7BDF73DCDB7F7997

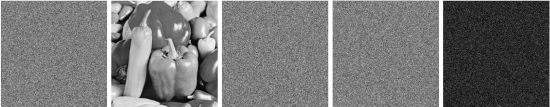
EFFA8BFF5DFgB7356BEEBgD7BB ；然后，对算法的加密过程进行敏感性测试：分 别利用密钥ko 、ki 对明文图像“Peppers”加密，得到密文图像co 与ci ，再获取co 与 ci 之间的差值 Co  ci ，所得结果如图 4-8 所示；最后，对算法的解密过程进行敏感性 测试：分别利用密钥KO 、ki 与K2 对密文图像CO 解密，得到解密结果D, 、Di 与D2 ， 再获取Di 与D2 之间的差值 IDi  D2 ，所得结果如图 4-9 所示。由图 4-8(d)可知，即使 密钥ko 与ki 之间的仅有 1 位比特值不同，利用它们加密所得的密文图像co 与ci 之间 也存在巨大差异，这表明加密算法的加密过程对密钥的变化十分敏感。由图 4-9(b)、(c)、

(d)可知，只有使用正确的密钥才能将密文图像恢复如初。另外， 由图 4-9(e)可以很容易 看出Di 与D2 之间存在很大的差异，这意味着 ISPD-IEA 的解密过程对密钥的变化也极 其敏感。



(a) 明文图像 (b) 密文图像 C0 (c) 密文图像 C1 (d) |C0 – C1 |结果 图 4-8 ISPD-IEA 加密过程的密钥敏感性分析

Fig. 4-8 Key sensitivity analysis of ISPD-IEA encryption process



(a) 密文图像 C0 (b) 解密结果 D0 (c) 解密结果 D1 (d) 解密结果 D2 (e) |D1-D2 |结果

图 4-9 ISPD-IEA 解密过程的密钥敏感性分析

Fig. 4-9 Key sensitivity analysis of ISPD-IEA decryption process

另外，本节还使用了比特变化率(NBCR)来定量地评估密钥的敏感度，其中 NBCR 的 计算方式如下：

 (4-6)

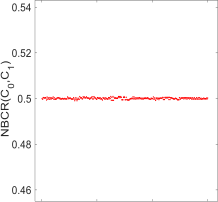
其中，H 与H2 是两组长度为LH 的序列，HammingH,H2 为计算H 与H2 对应位置的 不同字符的个数。一般地，若两组序列间的 NBCR 计算结果接近 0.5，则表明它们之间 无关联。

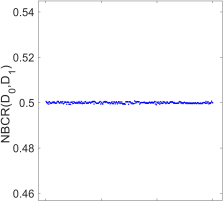
对密钥所有的比特值进行测试，测试过程为：首先，使用初始密钥ko 对图像“Peppers ” 加密，得到加密结果CO ；然后，分别改变密钥KO 的每一位比特值后得到新的密钥K1 ，

再利用k1 对图像“Peppers”加密，获得加密结果c ，并计算每次所得的co 与c1 之间 的 NBCR 值，由于密钥长度为 300 位，因此该过程需进行 300 次，图 4-10(a)展示了加密 过程中的 NBCR 测试结果；最后，利用密钥KO 对CO 解密，得到解密结果Do ，再分别改 变密钥ko 的每一位比特值后得到相应的新的密钥k1 ，再利用ki 对图像“Peppers ”解密， 得到解密结果D ，并计算每次所得的D, 与D 之间的 NBCR 值，同样地，该过程需进行 300 次，图 4-10(b)展示了密钥在解密过程中的 NBCR 测试结果。由图4-10 可以看出，密 钥在加密过程与解密过程的 NBCR 测试结果均接近期望值 0.5，也就是说，在算法的加

44

中国知网 https:iiwww.cnki . net

密与解密过程中，即使密钥发生的变化仅为 1 位比特值，所产生的后果也将截然不同。 这表明 ISPD-IEA 对密钥的变化极其敏感。



(a) 加密过程 NBCR 测试结果 (b) 解密过程 NBCR 测试结果

图 4-10 NBCR 测试结果 Fig. 4-10 NBCR test results

表 4-6 ISPD-IEA 对不同图像的 与 测试结果

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Lena | 5.1.09.tiff | Tank | Cameraman |
|  | 99.6039% | 99.6053% | 99.6082% | 99.6029% |
|  | 33.4617% | 33.4750% | 33.4489% | 33.4818% |

（5）抗差分攻击分析

本节选取“Lena”图像作为测试对象，将图像中位置为（1,1）的像素值增加 1 ，获 得一幅新的图像。利用 ISPD-IEA 分别对“Lena ”原图与新的图像加密，获得两幅密文 图像。最后， 再根据式(3-9) ~ (3-11)计算两幅密文图像的 *NPCR* 与 *UACI* 值。此外， 本节 还选取了多幅图片进行了抗差分攻击分析测试，测试结果如表 4-6 所示。根据表 4-6 所 展示的测试结果，不难看出，ISPD-IEA 对不同图像的测试结果均与理论值较为接近，这 表明该算法能够抵御差分攻击。

（6）对比分析

为了更好地说明 ISPD-IEA 的加密能力，本节将它与一些优秀的图像加密算法进行 了对比。表 4-7 列出了ISPD-IEA 和其它加密算法加密尺寸为 的“Lena ”图像 对应的安全分析结果，包含信息熵、*NPCR*、*UACI* 与相关系数。从表 4-7 可以看出，ISPD- IEA 的各项安全测试结果均为最优值。因此，相比于表中所示的其它图像加密算法，ISPD- IEA 具备更高的安全性能。

表 4-7 ISPD-IEA 与其它加密算法的安全测试结果对比

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 算法 | 信息熵 | NPCR | UACI | 相关系数 | | |
| 水平 | 垂直 | 对角 |
| 标准理论值 | 8 | 99.6094% | 33.4635% | 0 | 0 | 0 |
| ISPD-IEA | 7.9974 | 99.6039% | 33.4617% | 0.0026 | 0.0036 | -0.0033 |
| 文献[12] | 7.9969 | 99.5817% | 33.5412% | 0.0023 | 0.0036 | 0.0019 |
| 文献[61] | 7.9969 | 99.1547% | 33.2072% | 0.0068 | -0.0030 | -0.0474 |
| 文献[65] | 7.9893 | 99.5500% | 33.3800% | 0.0031 | -0.0033 | 0.0002 |
| 文献[66] | 7.9963 | 99.6137% | 33.4864% | -0.0083 | 0.0040 | -0.0463 |

**4.5** **本章小结**

本章提出了一种基于索引的同步置乱-扩散图像加密算法（ISPD-IEA）。首先，基于 普通的 Price 函数提出了一种 2D-Price 映射，该映射在大范围参数下处于超混沌状态。 然后，基于 2D-Price 映射进一步设计了出 ISPD-IEA 。该算法将置乱与扩散过程结合为 一个整体，使其能够在改变图像像素位置的同时扩散图像像素的微小变化。所提出算法 拥有简单的组成结构以及连贯的加密过程。最后，经各项性能评估测试结果表明，具有 较强的抗差分攻击能力与极高的加密效率。

**第五章** **基于忆阻超混沌正弦映射的图像加密算法**

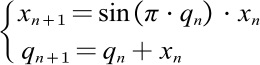
本章提出了一种忆阻超混沌正弦映射的图像加密算法（MHSM-IEA）。首先，将一 维 Sine 映射与忆阻器进行耦合，得到一个二维忆阻超混沌正弦映射（2D-MHSM）。然 后，利用 2D-MHSM 设计 MHSM-IEA。该算法采用了经典的置乱、扩散结构，其中，置 换过程使数字图像的像素排列无序，扩散过程借助一种基于比特的双环移位异或机制将 原始图像的微小变化传播到整个密文图像。最后，对算法的加解密效果进行了数值研究， 并对 MHSM-IEA 的安全性进行了充分评价。实验测试结果表明，MHSM-IEA 具有较好 的安全性、鲁棒性和较好的抗差分攻击能力，有利于提高图像信息的安全性。

**5.1** **二维忆阻耦合超混沌映射的设计与分析**

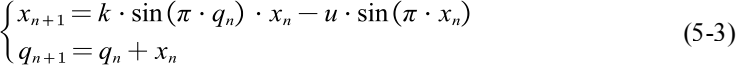
Sine 映射作为最常见的混沌映射之一，许多学者在此基础上提出了新的混沌系统。 忆阻器是一种具有记忆特性的非线性元件，可以与各种现有的动态电路和非线性系统相 结合，产生复杂的混沌振荡。在本节中， 我们研究了二维忆阻耦合超混沌映射，并探讨 了新系统的复杂动力学特性。

对于一维的混沌映射，其本质为状态变量xi  1 与其前一次状态变量xi 之间的迭代关 系，一维 Sine 映射状态变量间的迭代关系如式(5-1)所示：

xi  1  μsin(m · xi) (5-1) 其中，μ 为常量参数。虽然一维混沌系统的结构简单并且能够在一定条件下表现出混沌 行为，但低维混沌系统普遍存在一些不足之处，如混沌范围窄、混沌行为简单、Lyapunov 指数小等。文献[67]将一维 Sine 混沌系统与一个非线性的忆阻系统进行耦合，可得到一 个具有更复杂动态行为的 Sine 忆阻耦合系统，具体如式(5-2)所示。

 (5-2)

根据文献[67]所提供的设计思路，本章将式(5-1)与式(5-2)中所对应的 Sine 映射与忆 阻器进行耦合，得到了一个新的二维忆阻耦合超混沌映射（2D-MHSM），其定义如下式：

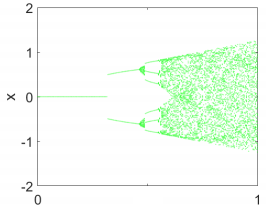


其中，*u* 与 *k* 为常量控制参数，并且 *k* 为 Sine 忆阻器的耦合强度，*x* 与 *q* 为状态变量。 图 5-1 为 2D-MHSM 在xo  0 . 5 , qo  0 . 5 , k  0 . 5 , u  [o,1] 时所对应的分岔图。图 5-2 与 5-3 分别展示了当xo  0 . 5 , qo  0 . 5 , k  0 . 5 , u  [o, 11 与xo  0 . 5 , qo  0 . 5 , *u* = 0.7, k  [-1.5 , 1 . 5] 时 2D-MHSM 对应的 Lyapunov 指数图。从图 5-3 中可以看出，

47

中国知网 https:iiwww.cnki . net

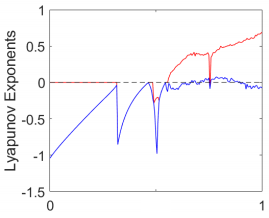
系统能够在较大范围内处于混沌状态，并且当 *k* 在[0.6, 0 . 8] 与 [-0.8 , - 0.6] 时，系统 存在超混沌现象。图 5-4 为 2D-MHSM 在xo  0 . 5 , qo  0 . 5 , *u* = 0.7, *k* = 0.5 的混沌轨迹 图，并且从该图中可以看出，2D-MHSM 在相空间内的运动轨迹是无序的，这表明此时 系统处于混沌状态。



u

图 5-1 2D-MHSM 分岔图

Fig. 5-1 The bifurcation diagram of 2D-MHSM



u

图 5-2 2D-MHSM 的混沌吸引子图

Fig. 5-2 The chaotic attractor diagram of 2D-MHSM

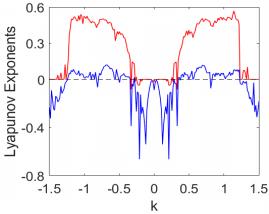


图 5-3 2D-MHSM 的 Lyapunov 指数图

Fig. 5-3 The lyapunov exponent diagram of 2D-MHSM

qi

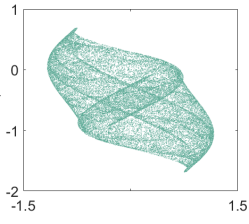
*x*i

图 5-4 2D-MHSM 的混沌吸引子图

Fig. 5-4 The chaotic attractor diagram of 2D-MHSM

表 5-1 2D-MHSM 生成的二进制序列的 NIST SP800-22 测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| 子测试 | | P 值 (≥0.01) | 结果 |
| 单比特频率 | | 0.8119 | 通过 |
| 频率块 | | 0.5874 | 通过 |
| 游程 | | 0.8118 | 通过 |
| 最长游程 | | 0.8720 | 通过 |
| 二进制矩阵秩 | | 0.1562 | 通过 |
| 离散傅氏变换 | | 0.5423 | 通过 |
| 非重叠模板匹配 | | 0.8136 | 通过 |
| 重叠模板匹配 | | 0.1826 | 通过 |
| 通用统计 | | 0.8293 | 通过 |
| 线性复杂度 | | 0.0921 | 通过 |
| 随机游动 | | 0.7277 | 通过 |
| 随机游动状态频数 | | 0.5197 | 通过 |
| 近似熵 | | 0.8596 | 通过 |
| 序列测试 | P 值 1 | 0.7544 | 通过 |
| P 值 2 | 0.4331 | 通过 |
| 累加和 | 正向 | 0.9117 | 通过 |
| 反向 | 0.9996 | 通过 |

为验证 2D-MHSM 所生成的混沌序列是否达到信息加密的标准，本节采用 NIST SP800-22 测试方法对 2D-MHSM 生成的混沌序列进行随机性测试，测试结果如表 5-1 所 示。由表 5-1 可知，2D-MHSM 所生成的混沌序列通过了所有子测试，这表明该混沌序

列具备良好的随机特性，适合应用于信息加密领域。

**5.2** **图像加密算法介绍**

为更好地保障图像的信息安全，本节基于 2D-MHSM 设计了一种新的图像加密算法 （MHSM-IEA），其加密过程如图 5-5 所示。首先，通过密钥生成 2D-MHSM 的初始参 数K ；随后，2D-MHSM 生成两组数量与明文像素总数相同的混沌序列用于算法的置乱 与扩散过程；最后，明文图像经两轮置乱、扩散操作后变为肉眼无法识别的密文图像。

|  |
| --- |
| 初始参数 |

|  |
| --- |
| 2D-MHSM |

|  |
| --- |
| 置乱 |

|  |
| --- |
| 扩散 |

|  |
| --- |
| 密钥 |

|  |
| --- |
| 混沌序列 |

|  |
| --- |
| 两轮 |

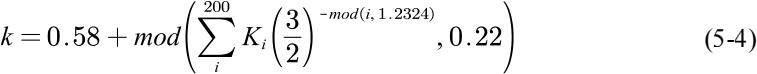
图 5-5 MHSM-IEA 的加密结构

Fig. 5-5 The encryption structure of MHSM-IEA

**5.2.1 算法的加密过程**

（1）混沌序列的生成

首先，将本算法中的密钥 *K* 设置成长度为 200 位的二进制序列，因此密钥空间为 2200 。然后，将 2D-MHSM 的初始状态值与初始参数分别设置为XO  0 . 5 ， o  0 . 5 ， u  0 . 7 ，再通过所设置的密钥获得 2D-MHSM 的初始参数 *k*，并且获取*k* 的具体方式如 式(5-4)所示。最后， 待所有初始条件确定后，2D-MHSM 将生成两组数量与明文像素总 数相同的混沌序列用于 MHSM-IEA 的置乱与扩散操作。



50

中国知网 https:iiwww.cnki . net

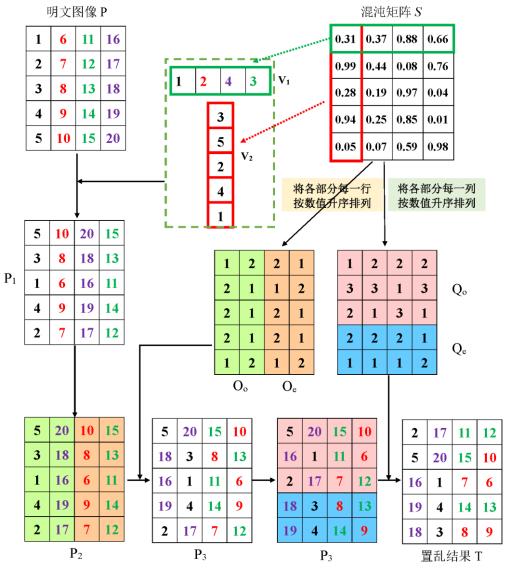


图 5-6 MHSM-IEA 置乱的演示

Fig. 5-6 Demonstration of MHSM-IEA permutation

（2）算法的置乱过程

一般来说，图像中一些高度相关的相邻像素可以赋予图像一些独特的像素排列特征， 但这些特征很容易被攻击者获取和识别。一般地，采用置乱操作可以打乱数字图像中所 有像素的排列位置，有效地降低了相邻像素之间的相关性。大多数置乱操作都是通过逐 行和逐列排序来打乱图像的像素位置。置乱后图像的像素分布可能具有一些明显的相关 性特征。本章设计了一种置乱方式能够交错打乱图像行和列的像素，置乱后图像的像素 分布没有明显的相关性特征，具体过程如下：

步骤 1 ：假设 *P* 为明文图像，并且 *P* 的大小为MXN ，利用 2D-MHSM 生成大小为 M  N 的混沌矩阵S 。

步骤 2 ：分别对S 的第一行与第一列序列值进行升序排列，获得索引向量vi 与V2 。 步骤 3：根据vi对P 进行列置乱，得到pi  {P(: , V, (1 , 1)) , P(: , V, (1 , 2)),… , P(: ,

51

中国知网 https:iiwww.cnki . net

V (1,N))} ,再根据V2对pi进行行置乱，得到P,  (P, (V2 (1 , 1)。:) , P, (V2 (1 , 2) , : ),…,P, ( V2 , (1 , M) , :)} 。

步骤 4：选择pi 的奇数列和偶数列，得到“奇部分”和“偶部分”，并将它们重组得 到P2 。然后对混沌矩阵S 的“奇数部分”和“偶数部分”按数值从小到大进行排序，得 到索引矩阵oo 和o e。

步骤 5：根据索引矩阵o. 和o e 对p2的像素进行置乱，得到p3，P3 (1 , :)  {p2 (1 , (o. ,

1)),… · , P2 (1 , O。(1 , i)) , P2 (1 , O e (1 , 1)),…,P2 (1 , o e (1 , j))},…,P3 (M, :)  P2 (M, (O。.(M, 1)) , …,P2 (M,O . (M, i)) , P2 (M, o e (M, 1)) , …,P2 (M, o e (M,j))} (i  j  N) 。

步骤 6 ：选择P3的奇数列和偶数列，得到“奇部分”和“偶部分”，并将它们重组得 到P4。然后对混沌矩阵S 的“奇数部分”和“偶数部分”按数值从小到大进行排序，得 到索引矩阵Qo和Qe 。

步骤 7：利用索引矩阵Q.和Qe置乱P4 的像素，得到置乱结果T ，T(: , 1)  {P4 (Q. (1 ,

1) , 1) , …,P4 (Q. (i, 1) , 1) , P4 (Qe (1 , 1) , 1) , · ,P4 (Qe (j , 1) , 1)} ,…,T(: , N)  {P4 (Q. (1 , N) , 1) , …,P4 (Q. (i.N) , N) , P4 (Qe (1 , N) , N),…,P4 (Qe (1 , N) , N)} (i  j  M) 。

为了更好地演示过程，图 5-6 给出了一个大小为5x4 的数字图像加密示例。

（3）算法的扩散过程

在 MHSM-IEA 的扩散过程中，本节提出了一种基于比特级的双循环移位异或扩散 机制。相较于常见的基于像素级的图像像素扩散方式，基于比特级的置乱方式能够在更 微观、更深层次上影响图像的像素。近年来， 越来越多的基于比特级的数字图像加密算 法被提出，并且它们通常是将十进制的图像像素序列转换成二进制的比特序列，再设计 出各类加密机制用于改变二进制比特序列。常见的基于比特级的加密机制主要包括循环 位移、DNA 编码以及异或运算等方式。然而， 这些方式均存在一些不足之处。对于基于 循环位移以及异或运算的加密机制来说，其加密过程过于简单且扩散效果差。一些基于 DNA 编码方式所设计的加密机制，其编码内容单一且实现过程较为复杂。为寻求一种 加密过程简单且安全性能良好的扩散机制，本节设计了一种基于比特级的双环移位异或 扩散机制，该机制通过对普通循环位移机制改进并结合了异或运算，最终能够轻易地实 现对图像像素的高安全性扩散操作。该扩散机制包含双循环移位过程与异或运算过程。 双循环移位过程如下：首先，将明文图像中每一行的像素转换为二进制像素比特序列。 然后，分别选取二进制像素比特序列中所有奇数与偶数位置的比特值，得到相应的奇数 序列与偶数序列。最后， 将奇数序列与偶数序列分别向不同的方向进行移位操作，并且 每一行的移位数与其对应的行数相同，得到新的二进制像素比特序列。异或运算过程为： 将双循环移位过程所得结果、上一行扩散操作结果以及混沌序列对应行的二进制混沌比 特序列进行异或操作，最终得到该行的扩散操作结果。

为便于理解扩散机制，本节提供了一个1x3 的像素矩阵加密示例，具体扩散过程如

52

中国知网 https:iiwww.cnki . net

图 5-7 所示。

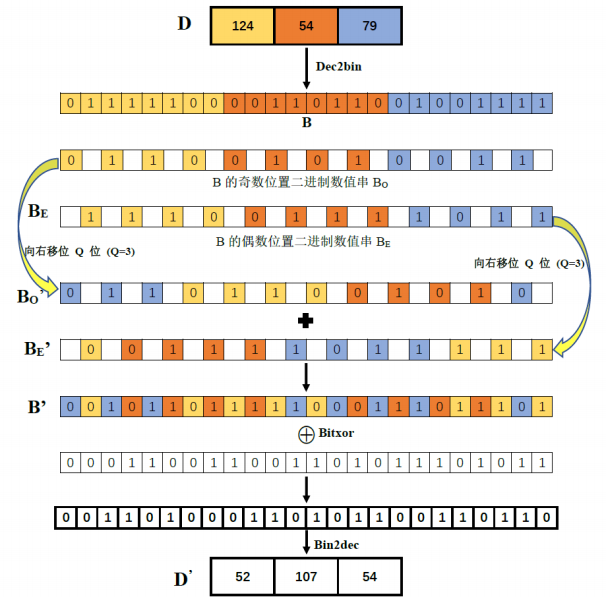


图 5-7 MHSM-IEA 扩散的演示

Fig. 5-7 Demonstration of MHSM-IEA diffusion

如图 5-7 所示，D 为密文图像的某一行像素，首先将 D 中所有的数值转为二进制， 得到二进制像素比特序列 B。其次，分别选取 B 中所有奇数位置与偶数位置的比特位， 得到Bo 与Be 。然后，分别将Bo 与BE 的所有比特位置视做一组循环圈，并且将Bo 与BE 分别沿顺时针与逆时针循环移位 3 位，得到Bo 与BE 。最后， 将Bo 与BE 重构为一个新 的二进制像素比特序列B，并且Bo 与BE 分别为B' 的奇数位置与偶数位置的值。将B  与 上一行扩散操作结果D · 1 进行异或操作，得到 D 所对应的双循环移位异或扩散结果X ， 再将X 转换为十进制结果D  。以上过程可由下式表示：

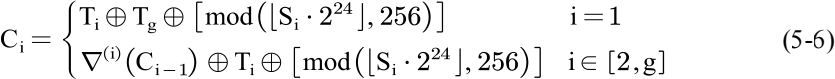
D   V(Y)(D) (5-5)

53

中国知网 https:iiwww.cnki . net

其中，Y 为循环移位的位数。

假设本章所提出算法中置乱操作的结果为T ，混沌矩阵为S ，并且它们的尺寸均为 M  N ，则本章所提出算法加密过程的扩散操作可由下式描述：



其中，“ a  b ”为对a 与b 进行异或操作， l」,为对 进行向下取整操作。扩散过程包括 两个部分：行扩散与列扩散。在进行行扩散时，式(5-6)中g  M ；在进行列扩散时，g  N 。

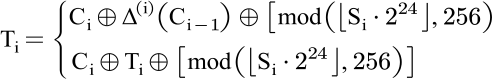
**5.2.2 算法的解密过程**

MHSM-IEA 的解密过程是其加密过程的逆操作。具体解密步骤如下：

步骤 1：根据密钥计算出 2D-MHSM 的一个初始参数K ，其计算方式如式(5-4)所示。

步骤 2 ：将 2D-MHSM 其它的初始条件设置为XO  0 . 5 ,q  0 . 5 ,u  0 . 7 ，使 2D- MHSM 生成两组数量与密文像素总数相同的混沌序列。

步骤 3：将步骤 1 生成的混沌序列分别组成两个与密文尺寸相同的混沌矩阵，并利 用它们进行两轮反扩散-反置乱操作。其中，反置乱操作是加密过程的置乱操作的逆过程， 反扩散过程可由下式描述：

   (5-7)

其中，C 为反置乱操作的结果，S 为混沌矩阵，反扩散操作结果为T 。 步骤 4：经过两轮反扩散-反置乱操作后，最终可获得解密图像。

**5.3** **实验仿真与性能分析**

本节通过在 Matlab2018b 仿真实验平台进行 MHSM-IEA 的加密仿真测试，并加密 了不同类型的图像，包括二值图像、灰度图像以及彩色图像等。另外， 本节还采用了多 种测量指标对 MHSM-IEA 的加密性能进行全面评估。

**5.3.1 仿真结果**

能够对不同类型的数字图像实现加密与解密是图像加密算法的基本要求，并且其解 密过程与加密过程所使用的密钥必须保持一致，否则解密失败。本节使用 MHSM-IEA 对 二值图像、灰度图像以及彩色图像进行加密与解密仿真， 其仿真结果如图 5-8 所示。仿 真结果表明，所有测试对象经 MHSM-IEA 加密后均成为无法获取任何信息的类噪声图 像，并且只能使用与加密过程相同的密钥才能将它们恢复如初。

54

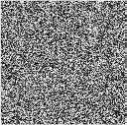
中国知网 https:iiwww.cnki . net

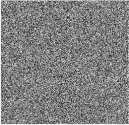


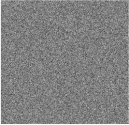




(a)明文图像









(b)密文图像







(c)解密结果

图 5-8 MHSM-IEA 对不同类型图像的加密仿真结果

Fig. 5-8 Simulation results of MHSM-IEA encryption for different types of images

**5.3.2 性能分析**

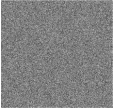
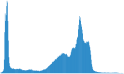
（1）直方图分析

图像直方图能够直观地展示出图像中各像素值的分布状况。由于图像的直方图只与 其像素组成相关，所以大多数图像的像素分布状况都各具特色，这导致攻击人员可通过 分析密文图像直方图的特征进而获知明文图像。因此， 对于一个加密性能优异图像加密 算法而言，其加密所得的密文图像各像素值出现频率相近，并且对应的直方图不具备明 显特征。本节选取的明文图像为“Cameraman”，“Peppers”，“Baboon ”，使用 MHSM-IEA 对它们加密并获得相应的加密结果。由图 5-9(b)可知，所有明文图像的直方图分布状况 各具特色，而对应密文图像的直方图（图 5-9(d)）分布状况都十分均匀且相似度极高。

图 5-9 展示了明文图像与密文图像以及它们对应的直方图。这表明 MHSM-IEA 能够有 效地隐藏图像的信息。

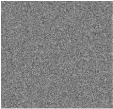
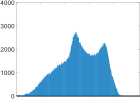
55

中国知网 https:iiwww.cnki . net

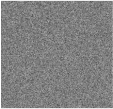
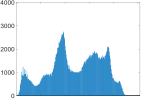


|  |
| --- |
|  |

|  |
| --- |
|  |



|  |
| --- |
|  |



|  |
| --- |
|  |

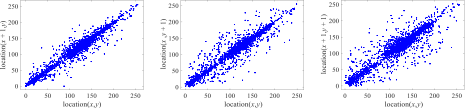


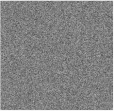
(a) 明文图像 (b) 明文图像直方图 (c) 密文图像 (d) 密文图像直方图

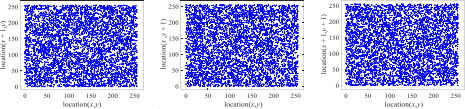
图 5-9 直方图分析

Fig. 5-9 Histogram analysis





(a) 明文图像 (b) 明文水平方向 (c) 明文垂直方向 (d) 明文对角方向



(e) 密文图像 (f) 密文水平方向 (g) 密文垂直方向 (h) 密文对角方向

图 5-10 “Cameraman”与其密文图像的相邻像素相关性

Fig. 5-10 Adjacent pixel correlation of plain and encrypted “Cameraman”

（2）相关系数分析

本节分别从图像“Cameraman”及其密文图像随机选取 3000 对相邻像素点并计算它 们在不同方向的相关系数。图 5-10 为图像“Cameraman ”加密前后的相邻像素分布图。

另外，表 5-2 给出了不同明文图像及其加密结果的相关系数。不难看出， 密文图像相邻 像素之间的相关系数低于明文图像相邻像素之间的相关系数。这表明，MHSM-IEA 加密 所得的密文图像具备较强的抗统计分析能力。

表 5-2 不同灰度图像加密前后的相关系数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 图像 | | 水平方向 | 垂直方向 | 对角方向 |
| Lena  (256  256) | 明文 | 0.9514 | 0.9246 | 0.9108 |
| 密文 | -0.0011 | -0.0014 | -0.0003 |
| 5.1.09.tiff  (256  256) | 密文 | 0.9364 | 0.9065 | 0.9011 |
| 密文 | 0.0009 | -0.0014 | -0.0010 |
| Lena  (512  512) | 明文 | 0.9536 | 0.9787 | 0.9421 |
| 密文 | -0.0021 | -0.0012 | 0.0004 |
| Cameraman  (512  512) | 明文 | 0.9910 | 0.9841 | 0.9743 |
| 密文 | 0.0014 | 0.0011 | -0.0020 |
| Peppers  (512  512) | 明文 | 0.9295 | 0.9650 | 0.9157 |
| 密文 | 0.0014 | 0.0012 | -0.0012 |

（3）信息熵分析

一般地，图像的信息熵值与其内部信息的不确定性及混乱程度呈正比关系，并且熵 值越高意味着获取到正确信息的难度越大。因此， 对于图像加密算法而言，其密文图像 的熵值应大于初始图像的熵值。图像的信息熵可根据式(3-8)计算获得。本发明对图像 “Tank”，“Car”，“Airplane”，“Boat”加密，并分别测试了各图像以及对应密文图像的 信息熵，所得结果如表 5-3 所示。

表 5-3 不同灰度图像加密前后的信息熵值

|  |  |  |
| --- | --- | --- |
| 图像 | 明文 | 密文 |
| Lena (256  256) | 7.4429 | 7.9976 |
| 5.1.09.tiff (256  256) | 6.7093 | 7.9976 |
| Lena (512  512) | 7.4451 | 7.9994 |
| Peppers (512  512) | 7.5973 | 7.9994 |
| Cameraman (512  512) | 7.0480 | 7.9994 |

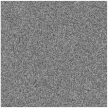
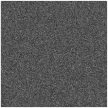
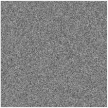
（4）密钥分析

对于一个图像加密算法而言，其密钥安全特性尤为重要，密钥安全特性包括密钥空 间与密钥敏感性两个方面。MHSM-IEA 的密钥是长度为 200 位的二进制序列，因此密钥

空间为 2200 ，这意味着该算法能够抵御穷举暴力攻击法。另外，本节以图像“Cameraman ” 为加密对象用于验证 MHSM-IEA 的密钥敏感性， 具体过程如下：设定初始密钥 K,  D47CE74F7F3FDD38BcgDFFBD3DBEBFFFFFF6DFC91D68E976F9 ，改变 密钥KO的第 1 位二进制值得到密钥ki  547CE74F7F3FDD38BcgDFFBD3DBEBFF FFFF6DFC91D68E976F9 ，再改变初始密钥KO 的第 50 位得到密钥ki  547CE74F 7F3FgD38BcgDFFBD3DBEBFFFFFF68E976F9 。图 5-11 展示了加密过程的密钥敏

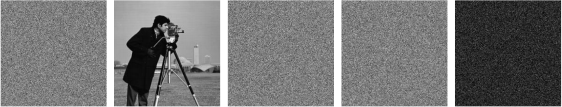
感性测试过程，图 5-11(a)为明文图像，5-11(b)、5-11(c)分别为使用初始密钥ko与密钥ki 对明文图像加密对应的密文图像c, 与ci，5-11(d)为c,与ci之间的差值。由 5-11(d)可知， 即使密钥K,与密钥ki之间的仅有一位不同，但使用它们加密所得结果之间差异巨大，因 此，MHSM-IEA 的加密过程对密钥极其敏感。本节还测试了MHSM-IEA 在解密时的密 钥敏感性，测试结果如图 5-12 所示，其中，图 5-12(a)为密文图像co，分别使用密钥ko、

ki与k2对co进行解密，解密结果分别为D,、Di、D2并如图 5-12(b)、(c)、(d)所示，显然， 只有使用密钥ko才能对密文图像实现解密。另外，图 5-12(e)给出了Di与D2之间的差异， 很明显，尽管ki与K2之间的差异很小，但它们对应的解密结果之间仍然有着天差地别， 这表明 MHSM-IEA 的解密过程同样对密钥极其敏感。



(a) 明文图像 (b) 密文图像 C0 (c) 密文图像 C1 (d) | C0 – C1 |结果 图 5-11 MHSM-IEA 加密过程的密钥敏感性分析

Fig. 5-11 Key sensitivity analysis of MHSM-IEA encryption process



(a) 密文图像 C0 (b) 解密结果 D0 (c) 解密结果 D1 (d) 解密结果 D2 (e) | D1 – D2 |结果

图 5-12 MHSM-IEA 解密过程的密钥敏感性分析

Fig. 5-12 Key sensitivity analysis of MHSM-IEA decryption process

下面将分别对 MHSM-IEA 加密过程与解密过程进行NBCR测试，并假设初始密钥 为ko，并且由上文可知ko是一组长度为 200 的比特序列。

加密过程的NBCR测试过程为：① 使用密钥KO对明文图像加密，加密结果为CO 。②

58

中国知网 https:iiwww.cnki . net

改变密钥ko的第i(i  1 , 2,…,200)位比特值得到ki，分别利用ki对明文图像加密，加密 结果为ci。③ 计算CO与ci(i  1 , 2,…,200)之间的NBCR值。加密过程的NBCR测试结果 如图 5-13(a)所示。

解密过程的NBCR 测试过程为：① NBCR使用密钥KO对CO解密，得到解密结果Do； ② 改变密钥ko的第i(i  1 , 2,…,200)位比特值得到对应密钥ki，分别利用密钥ki对co 解密，得到解密结果Di；③ 分别计算Do与Di之间的NBCR值。解密过程的NBCR测试结 果如图 5-13(b)所示。由图 5-13(a)可知，改变初始密钥的所有位置对应的NBCR值都接近 0.5，这意味着在 MHSM-IEA 的加密过程中，无论初始密钥发生任何变化，其加密结果 都与原加密结果没有关联。因此，MHSM-IEA 的加密过程对密钥的变化十分敏感。同理， 由图 5-13(b)可知，MHSM-IEA 的解密过程对密钥的变化也十分敏感。

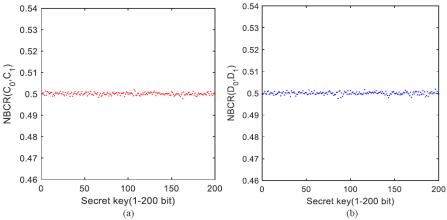


图 5-13 NBCR 测试结果 Fig. 5-13 NBCR test results

（5）差分攻击分析

差分攻击能够根据明文图像中选定像素的变化对加密结果所造成的影响来攻击加 密算法。改变明文图像的任意一个像素值，计算明文图像改变前后所对应的加密结果之 间的像素变化率(NPCR) 与像素变化强度(UAcn) ，具体计算方法如式(3-9) ~ (3.11)所示。 为确保测试结果更具普适性，本节利用 MHSM-IEA 对图像“Lena”，“Peppers”， “Cameraman”，“5.1.09.tiff”分别进行差分攻击测试，测试结果如表 5-4 所示。

表 5-4 MHSM-IEA 对不同灰度图像的差分攻击结果

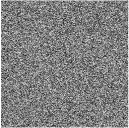
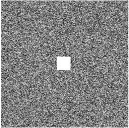
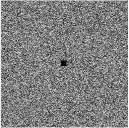
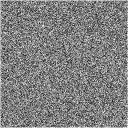
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 标准理论值 | Lena  (256  256) | 5.1.09.tiff  (256  256) | Peppers  (512  512) | Cameraman  (512  512) |
| NPCR | 99.6094% | 99.6078% | 99.6048% | 99.6082% | 99.6053% |
| UACI | 33.4635% | 33.4701% | 33.4780% | 33.4489% | 33.4750% |

由表 5-4 可知，即使测试对象完全不同，但所有的差分攻击测试结果均接近理论值， 这意味着 MHSM-IEA 具备较强的抗差分攻击能力。

（6）鲁棒性分析

图像加密算法应该忽略在不同设备之间传输数字图像时可能发生的任何负面影响， 如噪声或数据丢失。本节通过噪声攻击和数据丢失测试来验证 MHSM-IEA 的鲁棒性， 图 5-14 展示了测试结果。其中，图 5-14(a)与图 5-14(e)为明文图像“Lena”经 MHSM- IEA 加密所得的密文图像及其对应的解密结果，图 5-14(b)与 5-14(f)为1 . 1 %椒盐噪声的

密文图像及其解密结果，图 5-14(c)、(g)与图 5-14(d)、(h)分别为0 . 1526%与1 . 1%裁剪攻 击的密文图像及解密结果。由图5-14 可知，即使密文图像受到噪声或数据丢失的影响， 使用 MHSM-IEA 解密所得的图像仍然可以被大多数图像信息识别出来。



(a) 密文图像 (b) 1.1%椒盐噪声密文 (c) 0.1526%裁剪密文 (d) 1.1%裁剪密文



(e) 对(a)解密结果 (f) 对(b)解密结果 (g) 对(c)解密结果 (h) 对(d)解密结果

图 5-14 鲁棒性分析

Fig. 5-14 Robustness analysis

（7）算法计算复杂度与效率分析

MHSM-IEA 的运行过程主要包括混沌序列的生成、排列和扩散三个部分。对于大小 为M  N 的明文图像，第一部分需要生成两组长度为M  N 的混沌序列，对应的计算复 杂度为O(2  M  N) ；第二部分为置乱操作，计算复杂度为O(2  M  N) ；第三部分 为位异或运算和循环移位运算，前者的计算复杂度为O(8  M  N) ，后者的计算复杂度 为 o(2  M  N) 。由于该方法包含了两轮置换和扩散运算， 总 的计算复杂度为 o(26  M  N) 。此外，本节还利用MatlabR2018b 测试了加密系统的速度。实验设置 如下：实验设备配置 3.10 GHz@ CPU, 16GB 内存，Windows 10 操作系统。使用所提出 的算法对大小为256  256 的灰度图像进行加密，加密时间为 1.9660 秒。值得一提的是， 加密速度在一定程度上与运行环境和硬件设备有关。考虑到计算机中加密技术的快速发 展，提出的算法的加密速度也将得到提高。

60

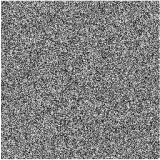
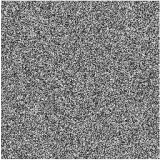
中国知网 https:iiwww.cnki . net

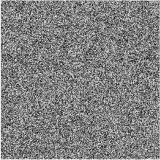
（8）对比分析

为了进一步说明 MHSM-IEA 的加密能力，我们将其加密测试结果与其他相关算法 进行了比较。表 5-5 列出了尺寸为256  256 的“Lena”图像的加密性能结果，并分析了 信息熵、NPCR 、UAcr以及相关系数等。由表 5-5 可知，与其他相关算法相比，MHSM- IEA 具备较小的相关系数以及较大的信息熵，并且NPCR和UAcr也更接近理论值。因此， MHSM-IEA 的加密算法也具有很高的安全性。

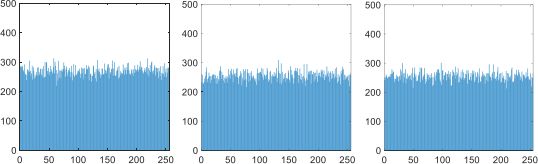
表 5-5 MHSM-IEA 与其它加密算法安全性测试结果对比

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 算法 | 信息熵 | NPCR | UACI | 相关系数 | | |
| 水平 | 垂直 | 对角 |
| 标准理论值 | 8 | 99.6094% | 33.4635% | 0 | 0 | 0 |
| MHSM-IEA | 7.9976 | 99.6078% | 33.4701% | -0.0011 | -0.0014 | -0.0003 |
| 文献[7] | 7.9975 | 99.6180% | 33.4960% | -0.0017 | -0.0084 | -0.0019 |
| 文献[61] | 7.9969 | 99.1547% | 33.2072% | 0.0068 | -0.0030 | -0.0474 |
| 文献[66] | 7.9963 | 99.6137% | 33.4864% | -0.0083 | 0.0040 | -0.0463 |
| 文献[68] | 7.9959 | 99.6200% | 33.4600% | 0.0019 | 0.0035 | 0.0008 |





(a) CMCT-IEA密文图像 (b) MHSM-IEA密文图像 (c) ISPD-IEA密文图像



(d) CMCT-IEA密文直方图 (e) MHSM-IEA密文直方图 (f) ISPD-IEA密文直方图 图 5-15 所提出的不同算法加密结果的直方图测试结果

Fig. 5-15 Histogram test results of the encryption results of the proposed different algorithms

另外，本节还将以上所设计的三种图像加密算法从算法安全性与效率进行对比。具

体测试过程为：分别使用 CMCT-IEA 、MHSM-IEA 与 ISPD-IEA 对尺寸为256  256 的 “Lena”图像加密，并对各加密结果的直方图、信息熵、 NPCR 、UAcr、相关系数以及 加密效率进行测试。图 5-15 展示了各算法加密结果的直方图测试结果。

如图 5-15 所示，本文所设计的三种图像加密算法均能有效地隐藏图像信息，并且它 们加密所得密文图像的直方图都趋于均匀。因此， 这三种图像加密算法具备良好地抵御 统计分析能力。

表 5-6 记录了 CMCT-IEA 、MHSM-IEA 与 ISPD-IEA 加密尺寸为256  256 的“Lena ” 图像的加密时间、信息熵、NPCR 、UAcr 以及相关系数测试结果。

表 5-6 本文提出的三种图像加密算法的加密性能对比

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | CMCT-IEA | MHSM-IEA | ISPD-IEA | 理论值 |
| 加密时间（秒） | | 0.205 | 1.966 | 0.093 | - |
| 信息熵 | | 7.9976 | 7.9976 | 7.9974 | 8 |
| NPCR | | 99.6039% | 99.6078% | 99.6048% | 99.6094% |
| UACI | | 33.4617% | 33.4601% | 33.4964% | 33.4635% |
| 相关系数 | 水平 | -0.0025 | -0.0011 | 0.0026 | 0 |
| 垂直 | 0.0020 | -0.0014 | 0.0036 | 0 |
| 对角 | -0.0003 | -0.0003 | 0.0036 | 0 |

由表 5-6 中所示的测试结果可知，CMCT-IEA 、MHSM-IEA 与 ISPD-IEA 的各项安 全测试结果均接近理论值。同时， 经比较分析可知，MHSM-IEA 在信息熵、*NPCR* 以及 相关系数等方面更接近理论值，CMCT-IEA 在 *UACI* 与对角方向的相关系数测试结果最 接近理论值，而 ISPD-IEA 的多数安全性测试结果均不如其它算法。另外，在加密效率 方面，不难看出，ISPD-IEA 的加密时间最短，其加密效率明显优于其它算法，尤其是 MHSM-IEA。因此可得出以下结论：MHSM-IEA 的安全性能最强但加密效率最低，ISPD- IEA 虽然安全性能较低却拥有极高的加密效率，而 CMCT-IEA 的安全性能与加密效率较 为均衡。

综上，本文所设计的三种图像加密算法均能有效地保护图像的信息安全，并且可根 据各自具备的特点应用于不同的加密场景。其中， MHSM-IEA 具备优异的安全性能，可 应用于国防、军事、科技等高级涉密型领域；CMCT-IEA 兼具良好安全性与加密效率， 适用于金融、医疗等专业应用型领域；而 ISPD-IEA 虽然安全性不如另外两个算法，但 极高的加密效率使得它能够应用于实时通讯、视频加密等信息处理量较大的使用场合。

**5.4** **本章小结**

为寻求一种具备高安全性的图像加密算法，本章提出了一种忆阻超混沌正弦映射的

图像加密算法（MHSM-IEA）。首先，本章设计了一个二维忆阻超混沌正弦映射（2D- MHSM），它由一个正弦映射和一个忆阻系统耦合而成。系统运行轨迹和 Lyapunov 指数 的测试结果表明，该混沌映射具有良好的遍历性和超混沌特性。然后， 基于 2D-MHSM 进一步设计出 MHSM-IEA。该算法主要包括置乱和扩散两个组成部分。其中，前者可以 有效打乱图像中的相邻像素，后者运用了一种新颖的基于比特的双环移位异或机制，能 够将明文图像的少量变化传递至整个加密图像。实验仿真与安全分析结果表明，该算法 能够加密各种类型的图像并且具备极高的安全性。最后，对本文所提出的三种图像加密 算法进行对比，总结了各算法的优劣，并根据对比的结果试分析了各加密算法设计结构 对加密性能的影响。

63

中国知网 https:iiwww.cnki . net

**第六章** **总结与展望**

**6.1** **研究工作总结**

随着互联网与多媒体信息技术的发展，数字图像作为一种重要的信息媒介在网络信 息交互的过程中发挥着重要的作用。然而，数字图像所存储的信息一般都为可视化信息， 这意味着任何获得该数字图像的人都可以直接地读取图片中的所有信息，很容易引起信 息泄露事故。近年来图像信息安全的保护引起了国内外学者的高度重视， 而传统的信息 加密技术显然无法满足加密图像的需求。因此，寻求出安全可靠的图像信息保护方法刻 不容缓。本文基于混沌理论与图像加密技术设计了三种混沌图像加密算法，并通过仿真 测试与安全性分析验证了它们的加密性能。以下将对本文所进行的主要研究工作进行总 结：

（1）提出了一种基于无平衡点混沌系统的混沌魔方变换图像加密算法（CMCT-IEA）。 首先，对现有的一个混沌系统进行改进，提出了一个新的无平衡点混沌系统并对其混沌 特性进行评估测试，测试结果也验证了该系统适用于混沌图像加密算法的设计。然后， 基于新的无平衡点混沌系统设计了一种混沌魔方变换图像加密算法，该算法拥有经典的 置乱、扩散加密结构，并且所有的加密过程均在三维空间内进行，这使其具备较好的加 密复杂度。最后，对其进行各项安全性分析测试，测试结果表明，该算法拥有良好的加 密性能。

（2）提出了一种 2D-Price 混沌映射的同步置乱-扩散图像加密算法。首先， 通过对 经典的 Price 映射的改进，得到了一个新的二维 Price（2D-Price）映射，该映射能够在 极大的参数范围内具备优异的超混沌特性。进一步地，设计了一种同步置乱-扩散图像加 密算法（ISPD-IEA），该算法能够在加密图像的过程中同时进行置乱与扩散操作。最后， 性能仿真与安全测试结果表明，ISPD-IEA 能够加密不同类型的数字图像，在通过各类 安全测试的前提下还能拥有极高的加密效率。

（3）提出了一种基于忆阻超混沌正弦映射的图像加密算法。首先，利用 Sine 映射 与一个忆阻器通过耦合的方式得到了一种二维忆阻超混沌正弦映射（2D-MHSM）。然后， 利用 2D-MHSM 设计了包含置乱和扩散过程的图像加密算法（MHSM-IEA）。为提升该 算法的安全性能，其扩散过程基于比特位面设计了一种的双循环移位异或机制，能够在 更微观的层面上将原始图像的微小变化传播到整个密文图像。最后，MHSM-IEA 的安全 性能测试结果也验证了其具备优异的安全性能。

通过对三种图像加密算法的比较分析可知，它们均能有效地保护图像的信息安全且 各具特点，可根据使用场景的需求从中选取最合适的加密方法。

64

中国知网 https:iiwww.cnki . net

**6.2** **未来工作展望**

本文立足于混沌图像加密技术，提出了三种较为新颖的图像加密算法，并且均具备 良好的加密性能。但是， 这些算法仍旧存在一些不足之处，需要进一步对其进行研究并 加以改善。未来可从以下几个方面开展研究工作：

（1）本文虽然能够基于现有的混沌系统改进出性能更优异的混沌系统，但对其混 沌性能的评估工作缺乏更全面的考虑。例如， 未能考虑到混沌系统因当前计算机精度不 足而产生混沌退化现象。

（2）当前研究内容的涉及领域单一，未来可深入研究其它领域内的相关知识并将 其与混沌图像加密技术相结合，进而拓展混沌图像加密领域的研究前景。例如，将量子 力学混沌图像加密技术结合，设计出性能更优异的加密算法。

（3）随着科技的发展，计算机信息处理能力不断增强，混沌图像加密算法的加密效 率定能得到有效提升。因此， 未来可将混沌图像加密算法广泛应用至音频、视频信息加 密领域。

（4）当前的研究进程仍处于仿真阶段，考虑到图像加密算法的实际应用价值，可将 本文所提出的混沌图像加密算法在移动应用平台得到工程实现。

65

中国知网 https:iiwww.cnki . net

**参考文献**

[1] Li P, Lo K T. A content-adaptive joint image compression and encryption scheme[J]. IEEE Transactions on Multimedia, 2018, 20(8): 1960-1972.

[2] DongY, Zhao G, MaY, et al. A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata[J]. Information Sciences, 2022, 593: 121-154.

[3] Lin H, Wang C, Cui L, et al. Brain-like initial-boosted hyperchaos and application in biomedical image encryption[J]. IEEE Transactions on Industrial Informatics, 2022, 18(12): 8839-8850.

[4] 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.

[5] 刘瀚扬,华南,王一诺,梁俊卿,马鸿洋.基于量子随机行走和多维混沌的三维图像加密算法[J]. 物理 学报, 2022, 71(17): 140-155.

[6] Wang X, Feng L, Zhao H. Fast image encryption algorithm based on parallel computing system[J]. Information Sciences, 2019, 486: 340-358.

[7] Alawida M, Samsudin A, Teh J S, Alkhawaldeh R S. A new hybrid digital chaotic system with applications in image encryption[J]. Signal Processing, 2019, 160: 45-58.

[8] Standard D E, et al. Federal information processing standards publication[J]. National Bureau of standrads, US Depratment of Commerce, 1977, 23.

[9] Stallings W. The advanced encryption standard[J]. Cryptologia, 2002, 26(3): 165-188.

[10] Wu Y, Noonan J P, Yang G, et al. Image encryption using the two-dimensional Logistic chaotic map[J]. Journal of electronic imaging, 2012, 21 (1): 013014.

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

[12] Wang X, Gao S,Ye X, et al. A new image encryption algorithm with cantor diagonal scrambling based on the PUMCML system[J]. International Journal of Bifurcation and Chaos, 2021, 31(01): 2150003.

[13] Wang B, Zhang B F, Liu X W. An image encryption approach on the basis of a time delay chaotic system[J]. Optik, 2021, 225: 165737.

[14] Hu M, Li J, Di X. Quantum image encryption scheme based on 2D Sine 2-L ogistic chaotic map[J]. Nonlinear Dynamics, 2023, 111(3): 2815-2839.

[15] Wang X, Li J, Yan H. An improved anti-quantum MST3 public key encryption scheme for remote sensing images[J]. Enterprise Information Systems, 2021, 15(4): 530-544.

[16] Zhou N, Pan S, Cheng S, et al. Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing[J]. Optics & Laser Technology, 2016, 82: 121-133.

[17] Chai X, Gan Z, Chen Y, et al. A visually secure image encryption scheme based on compressive sensing[J]. Signal Processing, 2017, 134: 35-51.

[18] Wei D, Jiang M. A fast image encryption algorithm based on parallel compressive sensing and DNA sequence[J]. Optik, 2021, 238: 166748.

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

[20] 王永, 李昌兵等. 混沌加密算法与 Hash 函数构造研究[M]. 北京: 电子工业出版社, 2011, 9: 5-6.

[21] Hosny K M, Kamal S T, Daewish M M, et al. New image encryption algorithm using hyperchaotic system and Fibonacci Q-Matrix[J]. Electronics, 2021, 10(9): 1066.

[22] Yu J, Xie W, Zhong Z, Wang H. Image encryption algorithm based on hyperchaotic system and a new

66

中国知网 https:iiwww.cnki . net

DNA sequence operation[J]. Chaos, Solitons & Fractals, 2022, 162: 112456.

[23] 孙克辉. 混沌保密通信原理与技术: Principle and technology of chaotic secure communication[M]. 北京: 清华大学出版社, 2015.

[24] Zheng J, Zeng Q. An image encryption algorithm using a dynamic S-box and chaotic maps[J]. Applied intelligence, 2022, 52: 15703-15717.

[25] Gao X. Image encryption algorithm based on 2D hyperchaotic map[J]. Optics & Laser Technology, 2021, 142: 107252.

[26] Lorenz EN. Deterministic nonperiodic flow[J]. Journal of atmospheric sciences, 1963, 20(2): 130-141.

[27] Matthews R. On the derication of a “chaotic” encryption algorithm[J]. Cryptologia, 1989, 8(1): 29-41.

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

[29] Jakimoski G, Kocarev L. Chaos and crytography: block encryption ciphers based on chaotic maps[J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2001, 48(2):163- 169.

[30] 黄润生, 黄浩等. 混沌及其应用[M]. 武汉: 武汉大学出版社, 2005.

[31] 廖晓峰, 肖迪, 陈勇, 等. 混沌密码学原理及其应用[M]. 北京: 科学出版社, 2009: 248.

[32] Mao Y, Chen G, Lian S. A novel fast image encryption scheme based on 3D chaotic baker maps[J]. International Journal of Bifurcarion and Chaos, 2004, 14(10): 3613-3624.

[33] Alvarez G, Li S J. Some basic aryptographic requirements for chaos-based cryphosystems[J]. International Journal of Bifurcarion and Chaos, 2006, 16(8): 2129-2151.

[34] Ozturk I, Sogukpinar I. Analysis and comparison of image encryption algorithms[J]. International Journal of Information Technology, 2004, 1(2): 108-111.

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

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

[37] Behnia S,AkhshaniA,AhadpourS, et al. A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps[J]. Physics Letters A, 2007, 66(4-5): 391-396.

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

[39] Liu L, Miao S. A new image encryption algorithm based on logistic chaotic map with varying parameter[J]. Springer Plus, 2016, 5(1): 1-12.

[40] Wang S, Peng Q,DuB. Chaotic color image encryption based on 4D chaotic maps and DNA sequence[J]. Optics & Laser Technology, 2022, 148: 107753.

[41] Lone P N, Mir U H. Image encryption using DNA coding and three-dimensional chaotic systems[J]. Multimedia Tools and Applications, 2022, 81(4): 5669-5693.

[42] Liu Z, Li J, Di X. A new hyperchaotic 4D-FDHNN system with four positive Lyapunov exponents and its application in image encryption[J]. Entropy, 2022, 24(7): 900.

[43] Cheng P, Yang H, Wei P, Zhang W. A fast image encryption algorithm based on chaotic map and lookup table[J]. Nonlinear Dynamics, 2014, 79(3): 2121-2131.

[44] Zhou N, Pan S, Cheng S, et al. Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing[J]. Optics & Laser Technology, 2016, 82: 121-133.

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

[46] Anwar S, Meghana S. A pixel permutation-based image encryption technique using chaotic map[J].

67

中国知网 https:iiwww.cnki . net

Multimedia tools and applications, 2019, 78(19): 27569-27590.

[47] XianY, Wang X, Yan X, LiQ, et al. Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion[J]. Optics and Lasers in Engineering, 2020, 134: 106202.

[48] Kumar CM, VidhyaR,BrindhaM. An efficient chaos based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function[J]. Applied Intelligence, 2022, 52 (3): 2556-2585.

[49] Hussain M, Iqbal N, Bashir Z. A chaotic image encryption scheme based on multi-directional confusion and diffusion operations[J]. Journal of Information Security and Applications, 2022, 70: 103347.

[50] Wang M, Wang X, Zhao T, et al. Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme[J]. Information Sciences, 2021, 544: 1-24.

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

[52] Xu L, LiZ, Li J, Hua W. A novel bit-level image encryption algorithm based on chaotic maps[J]. Optics and Lasers in Engineering, 2016, 78: 17-25.

[53] Wang T, Wang M. Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding[J]. Optics & Laser Technology, 2020, 132: 106355.

[54] Basha S M, Mathivanan P, Ganesh A B. Bit level color image encryption using Logistic-Sine- Tent- Chebyshev (LSTC) map[J]. Optik, 2022, 259: 168956.

[55] Gleick J. Chaos: making a new science[M]. Viking: 1987.

[56] Li T Y, Yorke JA. Period three implies chaos[J]. The American Mathematical Monthly, 1975, 82(10): 985-992.

[57] 向滔. 基于混沌的数字图像加密算法的分析与设计[D].重庆: 重庆大学,2014.

[58] Wolf A, Swift J B, Swinney H L. Determining Lyapunov exponents from a time series[J]. Physica D: nonlinear phenomena, 1985, 16(3): 285-317.

[59] Shannon C E. Communication theory of secrecy systems[J]. The Bell system technical journal, 1949, 28(4): 656-715.

[60] KerckhoffsA. La cryptographie militaire[J]. Journal des sciences militaires, 1883, IX: 5-83.

[61] Özkaynak F. Brief review on application of nonlinear dynamics in image encryption[J]. Nonlinear Dynamics, 2018, 92(2): 305-313.

[62] Bassham III L E, Rukhin AL, Soto J, Nechvatal J R, et al. Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications[M]. National Institute of Standards & Technology, 2010.

[63] Price W L. A controlled random search procedure for global optimization[J]. The Computer Journal, 1977, 20(4): 367-370.

[64] Liu Q, Li P, Zhang M C, et al. J. A novel image encryption algorithm based on chaos maps with Markov properties[J]. Communications in Nonlinear Science and Numerical Simulation, 2015, 20(2): 506-515.

[65] 赵雨, 杨真, 雍江萍, 展爱云, 张跃进. 基于混沌映射的图像加密算法研究[J].华东交通大学学报, 2022, 39(06): 26-36.

[66] Zhang Y. The image encryption algorithm with plaintext-related shuffling [J]. IETE Technical Review, 2016, 33(3): 310-322.

[67] Bao H, Hua ZY, Li H Z, et al. Discrete memristor hyperchaotic maps[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 68(11): 4534-4544.

[68] Ali T S, Ali R. A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box[J]. Multimedia Tools and Applications, 2022, 81: 20585-20609.

68

中国知网 https:iiwww.cnki . net