中国知网 https:iiwww.cnki . net

**摘要**

随着信息安全意识的增强，数字图像加密技术的研究和应用受到了广泛关注。 特别是在保护个人隐私和传输安全中，图像加密技术发挥着越来越重要的作用。因 此，为了满足当今复杂多变的安全需求，本文将忆阻混沌系统与 SHA-3 相结合， 实现了一图一密的加密效果，提高了图像加密技术的安全性，并基于软件仿真平台 开发了相应的图像加密应用程序。

（1）设计了基于五维忆阻混沌系统和 SHA-3 的彩色图像加密算法。基于忆阻 器的数学模型构建了一个五维忆阻混沌系统，该系统对初值高度敏感，这一特性与 SHA-3 的强抗碰撞性相结合，使每张加密图片拥有唯一密钥。随后采用分组置乱、 双向扩散和 DNA 算法对彩色图像进行加密，使每次加密所产生的密文具有高度的 随机性和不可预测性。最后通过实验验证了该算法具备巨大的密钥空间、高度的密 钥敏感性以及较强的抗剪切攻击能力。

（2）设计了基于六维忆阻分数阶超混沌系统和 SHA-3 的灰度图像加密算法。 该算法结合忆阻器和微分算子构建了一个六维忆阻分数阶超混沌系统，该系统在 较大初始值空间内展现出了良好的超混沌特性。根据这一特性，使用 SHA-3 针对 不同的明文生成多样化的混沌序列，并与哈希值结合后应用于三维立体置乱和三 维斜向扩散过程中。通过分析算法的安全性指标，发现该算法的信息熵接近理想值， 抗差分攻击能力较强，相邻像素之间的相关性较低，使得图像信息更安全。

（3）开发了基于上述两种图像加密算法的图形用户界面，主要功能包括图像 加密和图像解密以及附加文件保存功能和应用初始化功能，提供了一个简洁且易 于操作的平台。

**关键词**

忆阻混沌系统；SHA-3；图像加密；置乱算法

-I-

中国知网 https:iiwww.cnki . net

**Abstract**

With the increased awareness of information security, the research and application of digital image encryption technology have garnered widespread attention. Image encryption technology, particularly, plays an increasingly critical role in the protection of personal privacy and secure data transmission. Therefore, in order to meet today's complex and evolving security requirements, this thesis combines memristive chaotic systems with SHA-3 to achieve a one-image, one-key encryption effect, enhancing the security of image encryption technology, and an image encryption application has been developed based on the software simulation platform.

(1) A color image encryption algorithm based on a five-dimensional memristive chaotic system and SHA-3 was designed. A five-dimensional memristive chaotic system is constructed based on the mathematical model of memristors, which is highly sensitive to initial values. This characteristic combined with the strong collision resistance of SHA-

3 ensures that each encrypted image has a unique key. The color image is then encrypted using block scrambling, bidirectional diffusion, and DNA algorithms, resulting in ciphertext with high randomness and unpredictability for each encryption. Finally, experiments confirm that the algorithm possesses a vast key space, high key sensitivity, and strong resistance to cropping attacks.

(2) A grayscale image encryption algorithm based on a six-dimensional memristive fractional-order hyperchaotic system and SHA-3 was designed. The algorithm constructs a six-dimensional memristive fractional-order hyperchaotic system by combining memristors and differential operators, which exhibits excellent hyperchaotic characteristics in a large initial value space. Utilizing this property, SHA-3 generates diverse chaotic sequences for different plaintexts, which are then combined with hash values and applied in the processes of three-dimensional block permutation and three- dimensional oblique diffusion. By analyzing the security indicators of the algorithm, it is found that the entropy of the algorithm is close to the ideal value, the resistance to differential attacks is strong, and the correlation between adjacent pixels is low, making

-II-

中国知网 https:iiwww.cnki . net

the image information more secure.

(3) A graphical user interface based on the aforementioned two image encryption algorithms has been developed, with primary functions including image encryption and decryption, as well as additional functionalities for file saving and application initialization, offering a streamlined and user-friendly platform.

**Keywords**

Memristive chaotic system; SHA-3; Image encryption; Scrambling algorithm

-III-

中国知网 https:iiwww.cnki . net

目 录

[第 1 章 绪论 1](#bookmark2)

[1.1 研究背景和意义 1](#bookmark3)

[1.2 国内外研究现状 2](#bookmark4)

[1.2.1 忆阻混沌系统在图像加密领域的现状 2](#bookmark5)

[1.2.2 安全哈希算法在图像加密研究的现状 3](#bookmark6)

[1.2.3 忆阻混沌系统与 SHA 结合的图像加密现状 4](#bookmark7)

[1.3 主要工作及内容安排 5](#bookmark8)

[第 2 章 基础知识及相关理论 6](#bookmark9)

[2.1 忆阻器理论基础 6](#bookmark10)

[2.2 混沌系统理论基础 7](#bookmark11)

[2.2.1 混沌系统的特征 7](#bookmark12)

[2.2.2 混沌系统的分析方法 8](#bookmark13)

[2.3 安全散列算法的基础理论 10](#bookmark14)

[2.3.1 SHA-3 算法概述 10](#bookmark15)

[2.3.2 SHA-3 算法的特点 10](#bookmark16)

[2.4 图像加密的安全性评估方法 11](#bookmark17)

[2.4.1 密钥空间 11](#bookmark18)

[2.4.2 密钥敏感性 11](#bookmark19)

[2.4.3 信息熵 11](#bookmark20)

[2.4.4 直方图 12](#bookmark21)

[2.4.5 卡方检验 12](#bookmark22)

[2.4.6 相邻像素相关性 12](#bookmark23)

[2.4.7 抗差分攻击 13](#bookmark24)

[2.5 本章小结 14](#bookmark25)

[第 3 章 基于五维忆阻混沌系统和 SHA-3 的彩色图像加密算法 15](#bookmark26)

[3.1 五维忆阻混沌系统的建模与分析 15](#bookmark27)

[3.1.1 忆阻混沌系统的建模 15](#bookmark28)

[3.1.2 平衡点与耗散性的分析 17](#bookmark29)

[3.1.3 Lyapunov 指数与分岔现象 18](#bookmark30)

[3.1.4 混沌序列的 NIST 测试 18](#bookmark31)

[3.1.5 调控混沌系统的初始值 19](#bookmark32)

[3.1.6 基于 DSP 平台的电路实现 20](#bookmark33)

[3.2 图像加密算法的设计与实现 22](#bookmark34)

[3.2.1 利用 SHA-3 生成初始值 23](#bookmark35)

中国知网 https:iiwww.cnki . net

[3.2.2 分组置乱算法的设计 23](#bookmark36)

[3.2.3 双向扩散算法的设计 25](#bookmark37)

[3.2.4 DNA 编解码与运算 26](#bookmark38)

[3.3 图像解密算法的设计与实现 29](#bookmark39)

[3.4 实验仿真与安全性分析 29](#bookmark40)

[3.4.1 加解密结果 29](#bookmark41)

[3.4.2 密钥空间分析 30](#bookmark42)

[3.4.3 密钥敏感性分析 31](#bookmark43)

[3.4.4 信息熵 32](#bookmark44)

[3.4.5 相关性分析 32](#bookmark45)

[3.4.6 抗差分攻击 34](#bookmark46)

[3.4.7 直方图分析 35](#bookmark47)

[3.4.8 卡方检验 35](#bookmark48)

[3.4.9 抗剪切攻击 36](#bookmark49)

[3.4.10 抗噪声攻击 36](#bookmark50)

[3.5 本章小结 37](#bookmark51)

[第 4 章 基于六维忆阻分数阶超混沌系统和 SHA-3 的灰度图像加密](#bookmark52)

[算法 38](#bookmark52)

[4.1 六维忆阻分数阶超混沌系统的构建与分析 38](#bookmark53)

[4.1.1 六维忆阻分数阶超混沌系统的建模 38](#bookmark54)

[4.1.2 平衡点与耗散性的分析 40](#bookmark55)

[4.1.3 Lyapunov 指数和分岔现象 41](#bookmark56)

[4.1.4 调控混沌系统的初始值 42](#bookmark57)

[4.2 图像加密算法的设计与实现 43](#bookmark58)

[4.2.1 三维结构构造 44](#bookmark59)

[4.2.2 SHA-3 哈希值的分配 44](#bookmark60)

[4.2.3 混沌序列的生成 45](#bookmark61)

[4.2.4 三维立体置乱算法的设计 46](#bookmark62)

[4.2.5 三维立体斜向扩散算法的设计 48](#bookmark63)

[4.3 图像解密算法的设计与实现 49](#bookmark64)

[4.4 实验仿真与安全性分析 50](#bookmark65)

[4.4.1 加解密结果 50](#bookmark66)

[4.4.2 密钥空间分析 51](#bookmark67)

[4.4.3 密钥敏感性分析 51](#bookmark68)

[4.4.4 相关性分析 52](#bookmark69)

[4.4.5 信息熵 54](#bookmark70)

[4.4.6 卡方检验 54](#bookmark71)

[4.4.7 直方图分析 54](#bookmark72)

中国知网 https:iiwww.cnki . net

[4.4.8 抗噪声攻击 56](#bookmark73)

[4.4.9 抗差分攻击 57](#bookmark74)

[4.4.10 抗剪切攻击 57](#bookmark75)

[4.5 本章小结 58](#bookmark76)

[第 5 章 图像加密应用程序设计与实验验证 59](#bookmark77)

[5.1 实现平台与界面设计 59](#bookmark78)

[5.1.1 实验平台的选择 59](#bookmark79)

[5.1.2 界面设计 59](#bookmark80)

[5.2 功能实现 61](#bookmark81)

[5.2.1 图像加密功能的实现 61](#bookmark82)

[5.2.2 图像解密功能的实现 62](#bookmark83)

[5.2.3 附加功能:文件保存和界面初始化 62](#bookmark84)

[5.3 实验验证与对比分析 63](#bookmark85)

[5.3.1 加密算法一致性验证 63](#bookmark86)

[5.3.2 算法安全性对比分析 65](#bookmark87)

[5.4 本章小结 66](#bookmark88)

[结论 67](#bookmark89)

[参考文献 69](#bookmark90)

中国知网 https:iiwww.cnki . net

**第** **1** **章** **绪论**

1.1 研究背景和意义

随着信息技术时代的快速发展，图像作为一种至关重要的信息传递媒介，在我 们的日常生活中占据着愈发重要的地位。然而，随之而来的是日益突出的图像隐私 和信息安全问题。在这一背景下，图像加密技术应运而生，成为保障图像信息安全 不可或缺的手段[1-3]。

在信息的传输和存储中，图像加密技术的应用是确保敏感信息不被未经授权 访问者获取的关键环节[4, 5]。过去的研究主要侧重于传统加密算法，但是由于图像 与纯文本加密不同，它的数据量相比于文字大大增加，而且像素之间有着较强的相 关性，需要将二维或三维的图像矩阵转化为一维矩阵进行处理，所以这些应用经典 文本加密的算法效率并不高，安全性也较差[6-8] 。这些传统算法的安全性逐渐受到 挑战，特别是在处理大量高维度、高分辨率图像时， 传统算法的效率也面临瓶颈。

在图像加密中，混沌系统因其对初始状态的高灵敏度、伪随机性、遍历性和非 周期性等多种特性而被称为理想的伪随机序列生成器[9-11] 。因此，研究人员将混沌 系统与图像加密结合起来，试图得到更安全的加密算法[12-16]。随着研究的深入，忆 阻器因其先天的非线性而逐渐出现在大众视野中，通过忆阻器得到的混沌系统往 往能展现出复杂的动力学行为和良好的伪随机特性。对于加密而言，忆阻混沌系统 具有较高的初值敏感性并能产生难以预测的混沌序列，这一特点为设计出更为安 全的加密算法增添了一份助力，从而被广泛应用于加密技术中，以提高加密安全性。

此外，安全散列算法 3（Secure Hash Algorithm 3 ，SHA-3）作为一种新的加密 标准，以其高安全性、高效率和抗攻击能力强被广泛关注[17-19]。SHA-3 在图像加密 中的应用能够提供更为坚固的加密保障，增强图像数据在传输过程中的防护能力。 通过 SHA-3 生成的哈希值可以用于生成加密算法的密钥或用于加密算法的置乱与 扩散中，从而显著增加破解的难度，提高了图像加密的安全性。

因此，为了满足当今复杂多变的安全需求，图像加密技术的创新和改进变得尤

-1-

中国知网 https:iiwww.cnki . net

为重要。本文深入探讨基于忆阻混沌系统和 SHA-3 的图像加密算法，通过结合哈 希算法的优越性能和忆阻混沌系统的随机性，提供一种更为安全可靠、高效灵活的 图像加密方案。此研究不仅丰富了图像加密技术的研究内容，还探索了结合两种不 同加密手段的新思路。这样的融合有助于提升加密算法的安全性，使其更好地适应 当今信息传输与存储的需求。

1.2 国内外研究现状

1.2.1 忆阻混沌系统在图像加密领域的现状

忆阻混沌系统作为一种新兴的物理模型，已成为近年来的一个热点领域。2010 年，文献[20]设计并实现了一款混沌电路，该电路是由电容、电感以及忆阻器相串 联构成的，通过对该电路进行详尽的探究，在示波器中成功捕获到了单涡卷混沌吸 引子。在后续的研究中，学者纷纷将忆阻器与混沌系统结合起来[21-24] 。2015 年， 文献[25]通过添加平滑的磁控忆阻器，提出了一种基于三维自治混沌系统的新四维 忆阻超混沌系统。文献[26]提出了一种变化性的局部有源忆阻器模型，并在一个简 易的混沌电路中进行了应用，分析表明，忆阻电路可以产生复杂的非线性动力学。

随着信息安全需求的日益增长，将忆阻混沌系统应用到图像加密领域正逐渐 受到学术界的重视[27-33]。文献[34]提出了一个四维忆阻超混沌系统，随后展示了如 何将其与动态脱氧核糖核酸（Deoxyribonucleic Acid ，DNA）加密技术结合，用于 彩色图像的加密工作，这种结合利用了超混沌系统对初始密钥很敏感的特点和具 有复杂的动态行为，使其在彩色图像加密领域表现出色。文献[35]提出了一种基于 物理忆阻器的新型四维混沌系统，并基于该忆阻混沌系统，提出了一种基于盒式打 乱法、逐位异或操作和伪随机数生成的新型安全彩色图像加密算法。文献[36]通过 自反馈和正弦变换连接两个不同的离散忆阻器提出了一种新型的二维混合双忆阻 器超混沌映射，增强了该映射的复杂性。随后基于该映射生成的超混沌序列， 提出 了伪随机数生成器和图像加密策略，以提升其实际应用价值。文献[37]为了提升混 沌系统的复杂度，提出了一种具有反馈忆阻器的 Lorenz-Stenflo 模型的新型五维分 数阶混沌系统，并利用该混沌系统中的随机数据信息进行多媒体加密处理。2022

-2-

中国知网 https:iiwww.cnki . net

年，王兴元教授及其团队解决了长期困扰混沌密码学领域的关键问题，在文献[38] 中提出了反动力学退化定理，验证了混沌流密码系统的安全性。通过对现有文献的 综合分析，可以看到忆阻混沌系统在图像加密领域的应用不仅可行，而且具有广泛 的研究前景和实际应用价值。

1.2.2 安全哈希算法在图像加密研究的现状

在图像加密研究领域，哈希算法主要被用于生成加密算法的密钥或作为伪随 机数生成器。由于其哈希值的不可预测性和高抗冲突性，哈希算法对于密钥生成提 供了强有力的安全保障[39-42]。例如， 文献[43]提出了一种基于哈希密钥的图像加密 算法，采用 SHA-1 算法生成用于加密和解密的对称密钥并引入了多个混沌映射。 文献[44]提出了采用自适应小波的数字图像加密算法，该算法采用自适应小波变换 对图像进行重构并应用块加密技术进行重新排列，并引入 SHA-1 算法到原始图像 中以生成密钥序列，用作循环加密过程的循环指标。在文献[45]中，一种基于用户 生物特征和混沌动力系统的图像加密方法被提出，该方法结合了 SHA-256 哈希函 数和锯齿形变换，其中 SHA-256 哈希算法用来生成生物特征和明文图像的哈希值。 文献[46]提出了基于 SHA-2 256 生成初值并通过单个替换盒（Substitution box）的 置换和替换的图像加密算法。

2004 年，王晓云教授在文献[47]中展示了一个消息摘要算法 5（Message Digest Algorithm 5，MD5）算法的碰撞案例，随后在文献[48]中研究证明了理论上 SHA-1 是可以被破解的。因此，应避免将这些算法应用于对安全性要求较高的领域。SHA- 2 虽然提高了抵抗碰撞攻击的能力，但仍然使用了类似 SHA-1 的设计原理，而 SHA- 3 采用了完全不同的设计原理。国内外研究者已经对 SHA-3 算法在图像加密中的 应用进行了研究，提出了一些基于 SHA-3 算法的图像加密方案。这些方案通常利 用 SHA-3 生成的哈希值来初始化加密过程中的密钥，或者与其他加密技术，如混 沌系统、DNA 编码技术等结合，以增强加密算法的复杂度和安全性。例如，文献 [41]将 SHA-3 哈希函数和两个混沌系统相结合，算法首先通过 SHA-3 处理明文以 获得 384 位的密钥流哈希值，利用 SHA-3 算法和混沌系统的敏感性实现一次性密 码本效果。文献[49]提出了一种结合 SHA-3 算法和基于 DNA 编码的图像加密算

-3-

中国知网 https:iiwww.cnki . net

法。该算法首先使用 SHA-3 生成哈希值以增强密钥的敏感性，然后通过混沌系统 和 DNA 编码对图像像素进行置乱和编码，最终实现高安全性和良好实时性的图像 加密。文献[50]通过结合Logistic 映射和 Sine 映射，设计了一个三维的新 Logistic- Sine 映射。为了增强与明文相关的密钥流， 构建了一种新的密钥获取模型，该模型 结合了 SHA-3 哈希函数和公钥 ElGamal 密码学，提出了一个具有非对称结构的新 图像加密算法。目前， SHA-3 算法在图像加密的研究仍在不断进展中，研究者正在 探索新的设计范式和优化策略，以期达到更高效率和更强安全性的平衡。

1.2.3 忆阻混沌系统与 SHA 结合的图像加密现状

忆阻混沌系统与哈希算法的结合，代表了图像加密领域的一种创新方向，利用 混沌系统的高度随机性和哈希算法共同增强加密算法的安全性。在研究现状方面， 主要集中在如何让忆阻混沌系统产生的混沌序列与哈希算法产生的哈希值协同工 作，从而设计出新颖的图像加密算法。文献[51]利用 SHA-512 哈希函数结合明文图 像对忆阻超混沌系统进行迭代，以生成密钥序列。紧接着， 通过对明文图像的每一 行和每一列进行置换和扩散操作，完成了加密过程，实现了一种基于忆阻超混沌系 统的新颖图像加密方案。文献[52]提出了一种新型四维混沌加密算法，采用基于磁 控忆阻器模型的混沌系统，通过哈希过程增强明文敏感性，并结合 S 盒及位异或 操作来改变并打乱像素值，以增强加密安全性。文献[53]提出了一种结合 MD5 和 SHA-256 哈希函数生成密钥的新型图像加密模型，通过 Arnold 变换和混沌映射打 乱原始图像，再经过 DNA 编码、三矩阵扩散和DNA 解码，实现了既增强加密效 果又保持密钥强度的目的。文献[54]提出了一种利用安全散列算法引入的微小扰动 改变忆阻器混沌系统参数的新型彩色图像加密系统。该系统通过混沌矩阵进行跨 平面置乱，并用混沌序列改变像素位置，再通过跨平面 DNA 突变扩散技术对置乱 图像的每个像素值进行扩散处理。文献[55]使用三值忆阻器构建了一个超混沌系统， 并通过超混沌同步技术传输密钥信息。加密过程包括利用明文图像哈希值生成初 始密钥，以及基于哈希值和超混沌序列的像素和比特置乱操作，接着通过希尔伯特 曲线与密文反馈实现扩散。这些方法不仅增加了加密过程的随机性，而且由于哈希 算法的抗碰撞性，使得加密过程对原始图像的微小变化极度敏感，这显著提升了算

-4-

中国知网 https:iiwww.cnki . net

法的抗差分攻击能力。

在图像加密领域，忆阻混沌系统与哈希算法的结合已展现出显著的潜力，特别 是在生成难以预测的密钥序列和提升对差分攻击的抵抗力方面。已有研究通过利 用哈希算法如 SHA-512 和 SHA-256 生成初始参数，并结合忆阻混沌系统进行图像 的置乱和扩散操作，增强了加密算法的安全性。然而， 随着密码学攻击技术的不断 进步，对于更高安全级别的需求促使我们探索更为先进的哈希算法。在本文中将忆 阻混沌系统引入到更为强大的 SHA-3 哈希算法中，以此来生成更复杂的密钥序列 来增强加密算法的安全性。综上所述，结合忆阻混沌系统与 SHA-3 算法的图像加 密技术仍有广阔的研究空间和应用潜力。随着相关技术的不断发展和完善，这一领 域有望产生更为安全、高效的图像加密解决方案。

1.3 主要工作及内容安排

在本论文中，深入探讨了利用忆阻器构建的混沌系统与 SHA-3 算法结合后在 图像加密领域的应用。本文的结构安排如下：

第 1 章，绪论：简要介绍研究背景及意义，并详细讨论了忆阻混沌系统与 SHA- 3 算法在图像加密中的应用现状，同时概述了本论文的主要工作及安排。

第 2 章，基础知识及相关理论：本章阐述了本研究所涉及的关键理论基础，为 后续的实验和分析工作打下坚实的基石。提供了忆阻器理论、混沌系统特征分析方 法、安全散列算法和图像加密的安全性评估方法等基础知识。

第 3 章，基于五维忆阻混沌系统和 SHA-3 的彩色图像加密算法：本章首先给 出忆阻混沌系统的数学模型及其分析，紧接着提出了一个利用 SHA-3 512 生成初 值的彩色图像加密算法。此外通过一系列的安全性测试来评估加密算法的性能。

第 4 章，基于六维忆阻分数阶超混沌系统和 SHA-3 的灰度图像加密算法：本 章对六维忆阻分数阶超混沌系统进行了建模与分析。在此基础上，提出了结合 SHA-3 的三维立体图像加密算法。最后通过实验结果验证算法的安全性。

第 5 章，图像加密应用程序设计与实验验证：在第 5 章中设计并实现了一个 图像加密应用程序，描述了实验平台、界面设计以及功能实现， 并进行了算法一致 性和安全性对比分析的实验验证。

-5-

中国知网 https:iiwww.cnki . net

**第** **2 章** **基础知识及相关理论**

2.1 忆阻器理论基础

在电路理论中，常见的四个核心变量包括电压（*v*）、电流（*i*）、电荷（*q*）和磁 通(*φ*)。它们相互间存在六种基础的相互作用原则：磁通是电压随时间积分的结果； 电荷是电流随时间积分的结果；电阻（*R*）揭示了电流与电压的依存关系；电感（*L*） 将电流与磁通量联系起来；而电容（*C*）则衔接了电压与电荷。这五个关系被广泛 认知，直到 20 世纪末，蔡少棠教授提出了六种关系中缺失的一环，即电荷和磁通 之间的相互作用，并以此定义了忆阻器作为第四类基本电路元件。

忆阻器是一种具备了记忆特性的无源二端元件，忆阻器的电阻值会随着电流或 电压的改变而变化。忆阻器的出现填补了电路理论中电荷与磁通关系的空白。如图 2-1 所示完整的展示了电路基本变量之间的相互关系。

d*q*=*i*d*t*

|  |
| --- |
| d*φ*=*v*d*t* |

|  |
| --- |
|  |

|  |  |
| --- | --- |
| 电容 d*q*=*C*d*v*    电阻 d*v*=*R*d*i* | 忆阻器 d*φ* =*M*d*q*    电感 d*φ*=*L*d*i* |

*φ*

*q*

*v*

*i*

图 2-1 电路变量基本关系

Fig.2-1 Basic relation of circuit variable

根据其动态响应的控制方式，忆阻器可分为磁控型和荷控型。理想状态下的数 学公式分别如式（2-1）和式（2-2）所示：

-6-

中国知网 https:iiwww.cnki . net

*i* = *W* (φ)*v* （2-1）

*v* = *iM* (*q*) （2-2）

式中 *W* (*φ*)——磁控忆阻器的忆导函数，且满足  *M* (*q*) ——荷控忆阻器的忆阻函数，且满足 

*φ* 、*q* ——分别为忆阻器内部磁通量和电荷； *i* 、 *v* ——分别为忆阻器的电流和电压。

2.2 混沌系统理论基础

混沌系统理论是研究动态系统在确定性条件下展现出的似乎是随机或不规则 的行为。即便这些系统的初始条件被精确控制，在某些非线性动态系统中也能观察 到复杂性的存在。混沌是非线性系统的一种固有属性，与随机性不同，混沌性的特 点在于系统的长期行为不可预测，而且对初始条件极其敏感，即使是微小的差异也 会随时间推移而显著放大，这就是所谓的“蝴蝶效应”。

2.2.1 混沌系统的特征

混沌系统的研究揭示了动态系统在特定条件下展现出的复杂行为，这种表现 在数学上是确定性的，但在实际观察中可能显得无规律且难以预测。混沌系统具有 以下几个显著特征：

（1）初值敏感性。即便是两个初值存在极其微小的变化，都能随时间扩大成 完全不同的系统行为。因此， 长期预测变得非常困难，但短期行为是可以确定的。

（2）遍历性。在有限时间内，其路径能够穿过混沌区域中的每一个状态点。

（3）有界性。混沌系统的动态虽然无法精确预见，但其活动仍在一个确定的 有界空间内进行，这块区域被称作混沌吸引域。混沌系统的运动轨迹无论如何变化， 都始终会局限于这个区域内。

（4）内在随机性。混沌系统由于其对初始状态极度敏感以及其结果的不确定 性，展现了本质上的随机行为，还揭示了混沌在局部的不稳定性。

（5）标度性。混沌系统在不规则运动中的有序态， 只要存在高精度的检测设

-7-

中国知网 https:iiwww.cnki . net

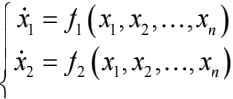
备或足够多精确的数据，就可以在不规则运动的区域内找到有序的运动状态。

2.2.2 混沌系统的分析方法

混沌系统的分析涉及到一系列数学和计算工具，用以理解和量化系统的动态 行为。以下是主要的分析方法，这些方法能够从不同角度探究混沌系统的内在特性， 揭示系统在不同参数条件下的复杂演化过程。通过这些方法的综合运用，混沌系统 的行为能够被准确地描述，为混沌理论在图像加密中的应用提供了坚实的基础。

（1）平衡点与稳定性

平衡点与稳定性是分析动力学系统特性的基础，尤其在混沌系统的研究中占 有重要地位。分析一个系统的平衡点及其稳定性是研究系统动力学特性的第一步。 在某种程度上，混沌系统的终态行为可以通过其平衡点来显现。因此，对系统的平 衡点进行计算和分析对混沌系统的性质分析至关重要。比如， 在一个*n* 维自治系统 的状态方程中，可表示为式（2-3）所示：

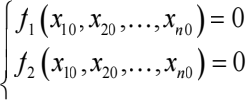


（2-3）

l*xn* = *fn* (*x*1, *x*2, … , *xn* )

系统的平衡点就是满足*f* (*x*) = 0 的那些点。如式（2-4）所示：

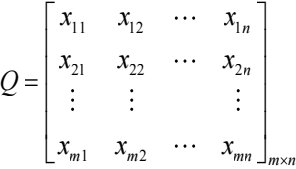


（2-4）



l*fn* (*x*10, *x*20, … , *xn*0 ) = 0

由此（2-4）可以得出混沌系统具有的 *m* 组平衡点如式（2-5）所示：

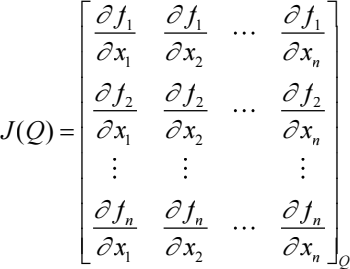


（2-5）

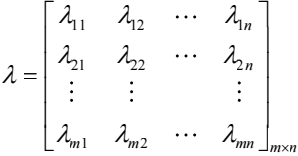
系统在平衡点处的雅可比矩阵如式（2-6）所示：

-8-

中国知网 https:iiwww.cnki . net

 （2-6）

使得特征方程 *J*(*Q*) − λ*E*= 0 ，解得 *m* 组特征值：

 （2-7）

根据各组平衡点对应的特征值，可以确定平衡点的类型。具体情况如下：

1) 渐进稳定结点：平衡点处的特征值均为负实数；

2) 不稳定结点：平衡点处的特征值都均为正实数；

3) 鞍点：平衡点处的特征值均为实数，且有正也有负时，平衡点一定是不稳 定的，这样的平衡点称为鞍点；

4) 鞍焦点：平衡点处的特征值既有共轭复数又有实数。

（2）Lyapunov 指数

李雅普诺夫指数是一种用来衡量动态系统中相邻轨迹分离速度的指标，反映 了系统对初始条件的敏感度，是混沌系统分析中的一个关键概念。如果系统存在正 的 Lyapunov 指数，则表示混沌特性。在这种情况下， 即使是微小的初始误差也会 随时间增长，导致预测变得非常困难。如果系统有多个正的 Lyapunov 指数，这可 能表明系统具有多个不稳定方向，导致更复杂的混沌行为，此时称为超混沌系统。

（3）相图

相图在混沌系统分析中是一种重要的工具，用于展示系统在相空间中的发展 曲线和动态行为。相图的形态和结构反映了系统的动态特性和混沌行为。在周期系 统中，相图可能呈现规则的周期结构或封闭的轨迹；而在混沌系统中，相图可能呈

-9-

中国知网 https:iiwww.cnki . net

现不规则的分布和复杂的形态，反映了系统的不可预测性和高度敏感性。

（4）分岔图

分岔图是动力学系统理论中的一个重要工具，它用于描绘一个系统状态随着 参数变化时所经历的定性变化。通过逐渐改变一个或多个系统参数，分岔图能够揭 示出系统随参数变化所经历的分岔点，这些分岔点是系统动态行为发生剧烈变化 的临界值。分岔图为理解复杂系统行为提供了直观的方式。

2.3 安全散列算法的基础理论

安全散列算法（Secure Hash Algorithm ，SHA）是一类密码学哈希函数，用于 将数据（如文件、消息或字符串等）压缩成一个固定长度的哈希值。SHA 算法的 主要目的是确保数据的完整性和安全性，即使数据发生了微小的改变，其哈希值也 会产生显著的变化。安全散列算法在数据传输、身份验证和数据完整性验证等方面 发挥着关键作用。安全散列算法的经典算法包括 SHA-1、SHA-256、SHA-512 等版 本，可以在实际应用中根据需要选择不同的输出长度和安全性级别。在图像加密领 域，安全散列算法通常用于生成密钥或作为加密算法的输入，使得加密算法的密钥 与明文自身相关，达到一次一密的效果。

2.3.1 SHA-3 算法概述

安全散列算法（SHA-3）在 2015 年被美国国家标准与技术研究院（NIST）正 式采纳作为联邦信息处理标准。在此之前，人们已经提出了很多针对 SHA-1 的攻 击方法。SHA-2 虽然提高了抵抗碰撞攻击的能力，但由于与 SHA-1 采用了相同的 Merkle–Damgård 结构，在理论上可能会受到相似的攻击。而 SHA-3 采用了与 SHA- 1 和 SHA-2 完全不同的设计原理，使用的是基于 Keccak 置换算法的海绵构造 （Sponge construction）。海绵构造通过吸收和挤压操作来处理数据， 能够更自然地 生成不同长度的输出，这种结构使得 SHA-3 在理论上对于某些类型的密码分析攻 击有更强的抵抗能力。

2.3.2 SHA-3 算法的特点

尽管 SHA-3 是作为 SHA 家族的一部分而开发的，但与 SHA-2 在设计上有根

-10-

中国知网 https:iiwww.cnki . net

本的不同。下面是 SHA-3 算法的一些主要特点：

（1）抗碰撞性。SHA-3 具有非常高的抗碰撞能力，意味着很难找到两个不同 的输入去生成相同的哈希值。

（2）抗预像攻击。SHA-3 算法非常难以找到与已知哈希值对应的原始数据， 这保证了数据的安全性，并且极大增强了抵抗预像攻击的能力，从而使得无论攻击 者拥有多少计算资源，都极难逆向推导出任何符合特定哈希输出的原始输入信息。

（3）随机性。SHA-3 算法的输出具有较高的随机性，即使输入的数据存在极 其微小的变化也会导致输出的哈希值存在显著的差异。这种随机性显著提高了攻 击者对哈希值预测的难度。

（4）高效率。与之前的哈希算法相比，SHA-3 在哈希速度和资源消耗方面表 现更好。它在硬件实现方面效率非常高，能够在较短的时间内处理大量数据。

（5）多输出长度。SHA-1 的散列长度为 160 位，而 SHA-3 能够提供多种不同 长度的输出，如 SHA-3 224, SHA-3 256, SHA-3 384, 和 SHA-3 512 这样用户可以根 据需要选择不同的安全级别。

2.4 图像加密的安全性评估方法

2.4.1 密钥空间

较大的密钥空间代表着更高的安全性，因为攻击者需要更多的尝试才能成功 破解密文。对于图像加密算法， 为了防止暴力破解攻击，评估其密钥空间的大小是 必要的，以确保其足够大。从密码学的角度出发，密钥空间的大小应该至少为2100 。

2.4.2 密钥敏感性

密钥敏感性是加密系统防御暴力攻击的另一个重要特征。在一个理想的加密 体系中，密钥的轻微变动应当引发加密图像呈现出截然不同的结果，且无法从加密 图像推导出原始或接近原始的密钥。

2.4.3 信息熵

信息熵是衡量信息不确定性的关键指标，经常用于评价加密图像的随机性，即 加密图像的像素分布的不确定性。信息熵可以通过以下公式（2-8）计算：

-11-

中国知网 https:iiwww.cnki . net

*H* = −Σlog2*P*（2-9）

式中 *P*(*si* ) ——像素*si* 出现的概率；

*n* ——像素的灰度级。

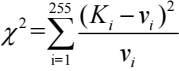
*n* = 256 的灰度图像，假设图像中的每个像素值都是完全随机的，得出信息熵为 8 是理论值。所以在图像加密中，密文图像的像素分布越接近随机分布，信息熵就 越接近 8 ，这表明加密过程有效地隐藏了原始图像的信息，提高了抗攻击的能力。

2.4.4 直方图

对于图像加密的安全性评估，直方图分析是一个重要的工具。因为它可以揭示 加密算法是否有效地混淆了原始图像的像素值分布。直方图具有直观、清晰的可视 化优点。通过直方图可以轻松地观察到各个灰度值的出现次数或频率。直方图越均 衡，就越难以通过统计方法分析，从而增加了破解的难度。

2.4.5 卡方检验

在图像加密的应用中，卡方检验是一种统计工具，用于检验加密图像的像素值 分布与理想的均匀随机分布之间的偏差程度。通过这种方法，可以量化图像加密后 的像素分布的随机性，如果像素值呈现出均匀分布，则表明攻击者难以从加密图像 中提取有用信息，进而增强加密算法的安全性。计算公式如公式（2-9）所示：

 （2-10）

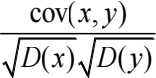
式中 *Ki* ——第*i* 个类别的实际频数； *vi* ——第*i* 个类别的期望频数。

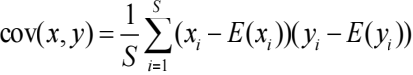
2.4.6 相邻像素相关性

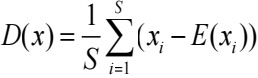
相关系数衡量了邻近像素之间的相互依存程度，相关性较高的相邻像素可能 会暴露出一些明文图像的结构或图案信息。因此，加密图像展现出的低相关性表明 加密算法对统计分析攻击拥有更强的抵御力。相邻像素的相关性计算如公式（2-10）、 （2-11）、（2-12）和（2-13）所示：

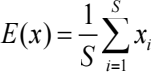
-12-

中国知网 https:iiwww.cnki . net

Y*xy* =  （2-11）

 （2-12）

 （2-13）

 （2-14）

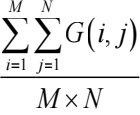
式中 *x* 、*y* ——两个临近像素点的像素值； *D*(*x*) 、*D*(*y*) —— *x* 、*y* 的方差；

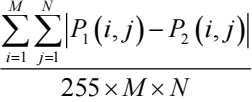
*E*(*x*) 、*E*(*y*) —— *x* 、*y* 的平均值；

*S* ——图像中选取的总的像素值。

2.4.7 抗差分攻击

差分攻击是一种密码分析技术，它通过分析对明文进行微小改变后密文的变 化情况，以此来猜测加密算法的某些内部特性，从而找出可能的密钥。为了评估图 像加密算法能否有效防御差分攻击，通常采用像素变化率（Number of Pixel Change Rate,NPCR）衡量单个像素在原图改变时密文图像的变动比例，以及采用平均像素 变化强度（Unified Average Changing Intensity, UACI）来计算原图某一像素变动引 起的密文图像像素强度的平均变化量。NPCR 和 UACI 的计算公式如式（2-14）和 （2-15）所示，理想值分别为 99.6094%和 33.4635%。

NPCR=  ×100% （2- 15）

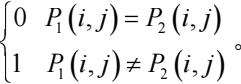
UACI =  ×100% （2- 16）

式中 *M* 、*N* ——图像的行数和列数；

-13-

中国知网 https:iiwww.cnki . net

*P*1 、*P*2 ——两幅图像在(*i*, *j* ) 位置的像素值；

*G* (*i*, *j* )——表示差异矩阵，且满足*G*(*i*, *j* )= 

2.5 本章小结

本章系统地介绍了本论文所依托的基础知识及相关理论，为后续章节中提出 的基于忆阻混沌系统和 SHA-3 的图像加密方法奠定了理论基础。本章首先讨论了 忆阻器的理论基础。随后， 深入探讨了混沌系统的相关理论，为理解混沌系统在图 像加密中的应用提供了必要的理论支持。紧接着，详细介绍了安全散列算法的概述 及其特点，突出了 SHA-3 在保障数据完整性和防护密码攻击方面的高效性和可靠 性，为图像加密提供了一个强有力的安全基础。最后， 详细讨论了图像加密的安全 性评估方法。这些评估方法为后续章节中对提出的加密算法进行安全性分析和效 果评估提供了标准和依据。

-14-

中国知网 https:iiwww.cnki . net

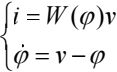
**第** **3** **章** **基于五维忆阻混沌系统和** **SHA-3 的彩色图像** **加密算法**

在本章中，首先对五维忆阻混沌系统进行数学建模和混沌特性分析，确保系统 动态行为的混沌性符合图像加密的需求。之后， 提出了一个图像加密算法，该算法 利用 SHA-3 512 生成混沌序列的初值，并通过分组置乱算法、双向扩散算法和 DNA 算法三个与混沌序列相关的操作进行加密。最后对密文图像的直方图、相关性、抗 噪声、信息熵、数据丢失和差分攻击等方面进行分析，结果表明本章提出的图像加 密方案具有较强的安全性。

3.1 五维忆阻混沌系统的建模与分析

3.1.1 忆阻混沌系统的建模

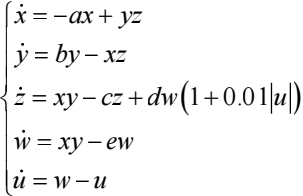
忆阻器具有非线性特性，可以为电子电路添加额外的功能。忆阻器是描述通量 *φ*和电荷*q* 之间关系的无源两端器件。本节中的忆阻器由磁通控制，流过器件的电 流与端口电压的关系可表示为：

 （3-1）

*W*(φ) = α+ βφ （3-2）

式中 *α* 、 *β*——忆阻器的内部参数。

将上述忆阻器模型的引入文献[56]所提出的四维系统中，构造了一个新型五维 忆阻混沌系统，系统表述如下：

 （3-3）

-15-

中国知网 https:iiwww.cnki . net

式中 *x* 、*y* 、*z* 、*w* 、*u* ——状态变量；

*a* 、*b* 、*c* 、*d* 、*e* ——系统参数。

设置忆阻混沌系统的参数*a* = 1.5 , *b* = 12 , *c* = 30 , *d* = 2 , *e* = 8.1005 ，初始状 态变量*x*0 = 1 , *y*0 = 1 , *z*0 = 1 , *w*0 = 1 , *u*0 = 1 ，令五维混沌系统迭代 500000 次，部 分平面的吸引子轨迹如图 3-1 所示。0-1 测试也是判断系统是否混沌的重要方法。 在参数和初值不变的情况下，令混沌系统迭代同样的次数，五维混沌系统的 0-1 测 试结果如图3-2 所示，运动轨迹为布朗运动。相图和 0-1 测试的结果均表明此时系 统展现为混沌状态。



10 1 5 20 25 30 35 40 45 X

5

a)*x-y* 平面相图

a) *x-y* plane phase diagram



|  |
| --- |
|  |

y

b)*y-w* 平面相图

b) *y-w* plane phase diagram

N

-30

|  |
| --- |
|  |

N

|  |
| --- |
|  |

25

35

45

5

y

c)*x-z* 平面相图 d)*y-z* 平面相图

c) *x-z* plane phase diagram d) *y-z* plane phase diagram

图 3-1 吸引子轨迹图

Fig.3-1 Attractor trajectory diagram

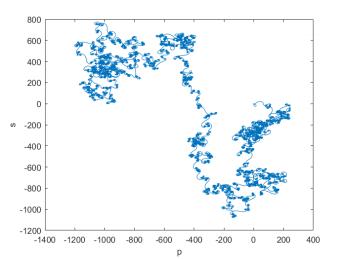
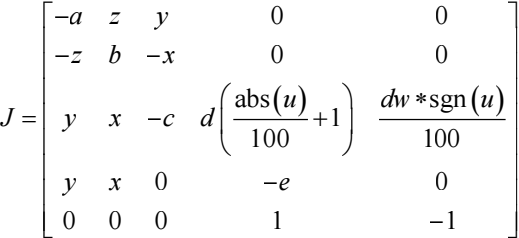


图 3-2 0-1 测试结果 Fig.3-2 0-1 test result

3.1.2 平衡点与耗散性的分析

系统（3-3）的雅克比矩阵为公式（3-4）所示：

 （3-4）

从系统（3-3）可以得到该忆阻混沌系统的平衡点 *S*0 = (0, 0, 0, 0, 0)。根据公式 （3-4），特征方程可得为(λ+1)(λ+ *e*)(λ+ *c*)(λ−*b*)(λ+ *a*) = 0 ，很容易得到λ1 = − 1 , λ2 =−*e* , λ3 =−*c* , *λ*4 = *b* , λ5 =−*a* 。因为系统参数*a* = 1.5 , *b* = 12 , *c* = 30 , *d* = 2 , *e* = 8.1005 ，所以得出*λ*1 , *λ*2 , *λ*3 , *λ*5 为负，*λ*4 为正，所以系统（3-3）有不稳定 的鞍点。系统（3-3）的散度为：

 = −*a* + *b* − *c* − *e* −1 （3-5）

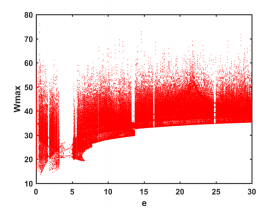
由于 −*a* + *b* − *c* − *e* −1 < 0，即系统（3-3）的散度值为负，可以据此得出结论， 该忆阻混沌系统具备耗散特性。

-17-

中国知网 https:iiwww.cnki . net

3.1.3 Lyapunov 指数与分岔现象

在其他参数和初值不变的条件下，令参数*e* 为控制变量，图 3-3 a)展示了系统 （3-3）随参数*e*∈[0,30] 变化的分岔图，而在相同条件下的李雅普诺夫指数谱如图 3-3 b)所示。从图3-3 b)中可以观察到系统（3-3）在大体上经历了由混沌到周期再 到混沌状态的转变过程，且大部分范围内系统表现出混沌状态，这与图 3-3 a)中所 展现的分岔图完全相符。这表明系统在参数*e* 变化时存在着周期性和混沌状态之间 的动态演变。



a) 随参数 *e* 变化的分岔图

a) Bifurcation diagram with parameter *e*

5

-25

-35

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

0 5 10 15 20 25 30 e

b) 参数 *e* 变化的 Lyapunov 指数

b) Lyapunov exponent with parameter *e*

图 3-3 分岔图和 Lyapunov 指数谱

Fig.3-3 Bifurcation diagram and Lyapunov exponent spectrum

3.1.4 混沌序列的 NIST 测试

为了确保序列的随机性，从而适用于加密应用，对混沌序列采用 NIST SP800- 22 标准检验。依据这一标准，如果序列的 P 值超过 0.01 ，表明它们没有可预测的 模式，满足了随机性标准[16, 57]。

与上文保持一致，也令系统参数*a* = 1.5 , *b* = 12 , *c* = 30 , *d* = 2 , *e* = 8.1005 ，初 始状态变量*x*0 = 1 , *y*0 = 1 , *z*0 = 1 , *w*0 = 1 , *u*0 = 1 。图 3-4 以图形方式直观展示了忆 阻混沌序列在各项随机性测试中的通过情况，从图中可以看出，15 种测试的 P 值 均大于 0.01，验证了其在安全应用中的有效性。这进一步证明了混沌系统在生成用 于加密算法的随机序列方面具有可靠性。

-18-

中国知网 https:iiwww.cnki . net

Q

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  | |  | | --- | | Y Z W U | | |  |
|  |
|  | |  | |

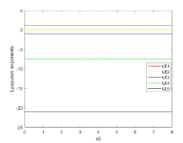
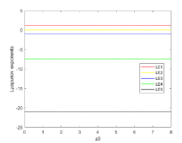
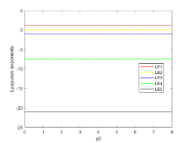
图 3-4 五维忆阻混沌系统的 NIST 测试

Fig.3-4 NIST test of five-dimensional memristive chaotic system

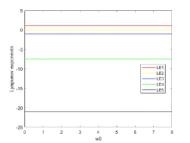
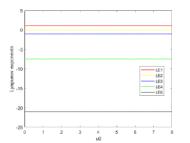
3.1.5 调控混沌系统的初始值

在图像加密应用中，系统的初始值必须具有高度的灵敏度和良好的调节性，以 确保加密过程的安全性和可靠性。因此，评估系统初值的可调节性对于保障加密强 度至关重要。为了评估系统初值的可调性，本研究在其他参数不变的情况下，让五 个初值参数分别在 0 至 8 的范围内变动，并计算相应的李氏指数。通过李氏指数， 我们可以量化系统对初值的敏感性和混沌特性的强度。

从图 3-5 可以发现李氏指数在整个调整范围内持续呈现正值，在此范围内系统 无论在何种初值下都能保持混沌状态。并确保了加密算法可以根据 SHA-3 的哈希 值输入不同的忆阻混沌系统初值生成多样化且难以预测的混沌序列，从而增强了 加密方案的安全性。



a) *x*0 ∈[0,8] b) *y*0 ∈[0,8] c) *z*0 ∈[0,8]



d) *w*0 ∈[0,8] e) *u*0 ∈[0,8]

图 3-5 随初始值变化的 Lyapunov 指数 Fig.3-5 Lyapunov exponent with initial value

3.1.6 基于 DSP 平台的电路实现

为了在工程应用中实现混沌系统，电路的实际搭建显得至关重要。本节利用基 于数字信号处理器（Digital Signal Processor ，DSP）的可编程硬件平台来检验忆阻 混沌系统的动态行为。详细的硬件架构展示在图 3-6 中。

通信接口

计算机

通道-1

数模转换器 （DAC8552）

示波器



数字信号

通道-2

DSP

(TMS320F28335)

图 3-6 DSP 的硬件架构图

Fig. 3-6 Hardware architecture diagram of DSP

本实验中，采用了 TMS320F28335 作为 DSP 芯片，并搭配 DAC8552 数模转换 器。首先进行的是对 DSP 的初始设定。接下来， 采用龙格-库塔法对连续混沌系统 进行离散化，获得如式（3-6）到（3-10）所示的迭代方程，并载入到 DSP 芯片中。 随后，DSP 对数据进行处理，并将处理结果发送到数模转换器，完成数字信号向模 拟信号的转换过程。通过这一系列步骤，能在数字示波器上直观观察到系统（3-3） 的运动轨迹，设置系统参数*a* = 1.5 , *b* = 12 , *c* = 30 , *d* = 2 , *e* = 8.1005 ，初始状态变 量*x*0 = 1 , *y*0 = 1 , *z*0 = 1 , *w*0 = 1 , *u*0 = 1 ，结果如图 3-7 所示。有效地验证了理论模

-20-

中国知网 https:iiwww.cnki . net

型与实际电路之间的一致性。

〔*K*11 = −*ax*(*i*) + *y*(*i*)*z*(*i*)

（3-6）





{





*K*21 = *by*(*i*) − *x*(*i*)*z*(*i*)

*K*31 = *x*(*i*)*y*(*i*) − *cz*(*i*) + *dw*(*i*)(1+ 0.01 *u*(*i*) ) *K*41 = *x*(*i*)*y*(*i*) − *ew*(*i*)

l*K*51 = *w*(*i*) − *u*(*i*)

〔*K*12 = −*a* (*x*(*i*) + 0.5*h* × *K*11) + (*y*(*i*) + 0.5*h* × *K*21)(*z*(*i*) + 0.5*h* × *K*31)



*K*22 = *b* (*y*(*i*) + 0.5*h* × *K*21) − (*x*(*i*) + 0.5*h* × *K*11)(*z*(*i*) + 0.5*h* × *K*31)

*K*32 = (*x*(*i*) + 0.5*h* × *K*11)(*y*(*i*) + 0.5*h* × *K*21) − *c* (*z*(*i*) + 0.5*h* × *K*31)





+ *d* (*w*(*i*) + 0.5*h* × *K*41)(1+ 0.01(*u*(*i*) + 0.5*h* × *K*51) )

{







（3-7）

*K*42 = (*x*(*i*) + 0.5*h* × *K*11)(*y*(*i*) + 0.5*h* × *K*21) − *e* (*w*(*i*) + 0.5*h* × *K*41)

l*K*52 = (*w*(*i*) + 0.5*h* × *K*41) − (*u*(*i*) + 0.5*h* × *K*51)

〔*K*13 = −*a* (*x*(*i*) + 0.5*h* × *K*12) + (*y*(*i*) + 0.5*h* × *K*22)(*z*(*i*) + 0.5*h* × *K*32)



*K*23 = *b* (*y*(*i*) + 0.5*h* × *K*22) − (*x*(*i*) + 0.5*h* × *K*12)(*z*(*i*) + 0.5*h* × *K*32)  *K*33 = (*x*(*i*) + 0.5*h* × *K*12)(*y*(*i*) + 0.5*h* × *K*22) − *c* (*z*(*i*) + 0.5*h* × *K*32) { + *d* (*w*(*i*) + 0.5*h* × *K*42)(1+ 0.01 (*u*(*i*) + 0.5*h* × *K*52) )

（3-8）

*K*43 = (*x*(*i*) + 0.5*h* × *K*12)(*y*(*i*) + 0.5*h* × *K*22) − *e* (*w*(*i*) + 0.5*h* × *K*42) l*K*53 = (*w*(*i*) + 0.5*h* × *K*42) − (*u*(*i*) + 0.5*h* × *K*52)



〔*K*14 = −*a* (*x*(*i*) + 0.5*h* × *K*13) + (*y*(*i*) + 0.5*h* × *K*23)(*z*(*i*) + 0.5*h* × *K*33)



*K*24 = *b* (*y*(*i*) + 0.5*h* × *K*23) − (*x*(*i*) + 0.5*h* × *K*13)(*z*(*i*) + 0.5*h* × *K*33)

*K*34 = (*x*(*i*) + 0.5*h* × *K*13)(*y*(*i*) + 0.5*h* × *K*23) − *c* (*z*(*i*) + 0.5*h* × *K*33)





+ *d* (*w*(*i*) + 0.5*h* × *K*43)(1+ 0.01 (*u*(*i*) + 0.5*h* × *K*53) )

{







（3-9）

*K*44 = (*x*(*i*) + 0.5*h* × *K*13)(*y*(*i*) + 0.5*h* × *K*23) − *e* (*w*(*i*) + 0.5*h* × *K*43)

l*K*54 = (*w*(*i*) + 0.5*h* × *K*43) − (*u*(*i*) + 0.5*h* × *K*53)

〔*x*(*i* +1) = *x*(*i*) + *h* / 6 × (*K*11+ 2*K*12 + 2*K*13 + *K*14)



*y*(*i* +1) = *y*(*i*) + *h* / 6 × (*K*21+ 2*K*22 + 2*K*23 + *K*24) 

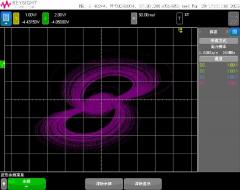
{*z*(*i* +1) = *z*(*i*) + *h* / 6 × (*K*31+ 2*K*32 + 2*K*33 + *K*34) 

（3-10）

*w*(*i* +1) = *w*(*i*) + *h* / 6 × (*K*41+ 2*K*42 + 2*K*43 + *K*44) l*u*(*i* +1) = *u*(*i*) + *h* / 6 × (*K*51+ 2*K*52 + 2*K*53 + *K*54)

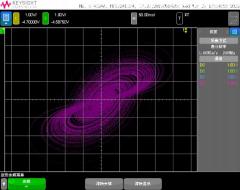
-21-

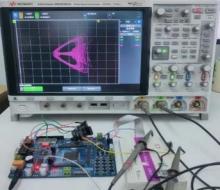
中国知网 https:iiwww.cnki . net





a)*x-y* 平面相图 b)*y-w* 平面相图

a) *x-y* plane phase diagram b) *y-w* plane phase diagram



c)*x-z* 平面相图 d)*y-z* 平面相图

c) *x-z* plane phase diagram d) *y-z* plane phase diagram

图 3-7 示波器上捕获的相图

Fig. 3-7 Oscilloscope-captured phase diagram

3.2 图像加密算法的设计与实现

本节提出的基于五维忆阻混沌系统和 SHA-3 的彩色图像加密算法，该算法包 括三个关键步骤：分组置乱、双向扩散和 DNA 算法。首先， 使用 SHA-3 算法对明 文图像生成 3 个 512 位的哈希值，这些哈希值不仅确保了加密过程的密钥唯一性， 而且为后续步骤生成五维混沌序列。随后明文图像的像素位置受到分组置乱的干 扰，紧接着通过双向扩散改变像素值。最后， 根据 DNA 算法再次改变像素值，生 成密文图像。加密的完整过程如图3-8 所示。

-22-

中国知网 https:iiwww.cnki . net

|  |
| --- |
| R |

|  |
| --- |
| B |

SHA-3

SHA-3

SHA-3

|  |
| --- |
| 分组置乱 |

|  |
| --- |
| 分组置乱 |

|  |
| --- |
| *k*1 |

|  |
| --- |
| *k*2 |

|  |
| --- |
| *k*3 |

|  |
| --- |
| **原始图像** |

|  |
| --- |
| G |

|  |
| --- |
| 混乱序列 |

|  |
| --- |
| 分组置乱 |

|  |
| --- |
| 双向扩散 |

|  |
| --- |
| 双向扩散 |

|  |
| --- |
| DNA加密 |

|  |
| --- |
| DNA加密 |

|  |
| --- |
| 双向扩散 |

|  |
| --- |
| DNA加密 |

|  |
| --- |
| **加密图像** |

图 3-8 彩色图像加密算法整体架构图

Fig. 3-8 Overall architecture diagram of the color image encryption algorithm

3.2.1 利用 SHA-3 生成初始值

通过在明文图像上应用 SHA-3 512 散列算法来创建加密密钥。因为 SHA-1 在 2017 年被 Google 破解，所以本章选择了 SHA-3 512。将明文图像 P 按照 R 、 G 和 B 分为灰度图像，分别对三个灰度图像应用 SHA-3 512 散列算法得到三个哈 希值*k*1 , *k*2 , *k*3 ，然后将生成的哈希值映射在 0 和 6 之间，使其适用于混沌系统， 作为混沌系统的初值， 其中 *x*0 = mod (*k*1 ,7) , *y*0 = mod (*k*2 ,7) , *z*0 = mod (*k*3 ,7) , *w*0 = mod (*k*1 + *k*2 ,7) , *u*0 = mod (*k*1 + *k*3 ,7) ，将参数 *a* = 1.5 , *b* = 12 , *c* = 30 , *d* = 2 , *e* = 8.1005 和初值代入系统（3-3）生成五维混沌序列*X*, *Y*, *Z*, *W*, *U*。

3.2.2 分组置乱算法的设计

本节详细介绍一种新颖的分组置乱过程。通过该置乱过程，明文图像的像素位 置被有效打乱。图 3-9 以 R 通道为例展示了置乱算法的实现过程，下面将详细描 述该置乱算法的步骤：

-23-

中国知网 https:iiwww.cnki . net