分类号 TP391.4　　密　　级

U D C　　学校代码 10500

湖北工業大學

HUBEI UNIVERSITY OF TECHNOLOGY

硕士学位论文

（全日制专业学位）

题　　目：基于超混沌系统的图像加密算法研究

英文题目：Research on Image Encryption Algorithm Based on Hyperchaotic System

学位申请人姓名：彭博

申请学位学科专业：计算机技术

指导教师姓名：张明武

二〇二〇年六月

分类号 TP391.4　　密　　级

U D C　　学校代码 10500

湖北工業大學

HUBEI UNIVERSITY OF TECHNOLOGY

硕士学位论文

题　　目 基于超混沌系统的图像加密算法研究

英文题目 Research on Image Encryption Algorithm Based on Hyperchaotic System

研究生姓名（签名）

指导教师姓名（签名）　　职　称 教授

申请学位学科名称 计算机技术　　学科代码 085211

论文答辩日期 2020.06.06　　学位授予日期

学院负责人（签名）

评阅人姓名 林莉　　评阅人姓名 饶泓

2020 年　6　月　22　日

湖北工業大學

学位论文原创性声明和使用授权说明

原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的研究成果。除文中已经标明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的研究成果。对本文的研究做出贡献的个人和集体，均已在文中以明确方式标明。本声明的法律结果由本人承担。

学位论文作者签名：彭博　　日期：2020　年 6 月 22 日

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，即：学校有权保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权湖北工业大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

学位论文作者签名：彭博　　指导教师签名：

日期：2020 年 6 月 22 日　　日期：2020 年 6 月 22 日

摘　　要

随着时代的发展和网络信息技术的进步，数字图像已成为人们获取信息的重要方式之一。尽管数字图像具有直观性强，方便快捷等特点，逐渐获得人们的青睐，但是其存在的安全隐患等问题也不能忽视。如何通过图像加密技术来保障图像的安全传输已成为当前研究的热点之一。数字图像具有有别于一维数据流的冗余度高、数据量大、像素相关性强等特点，因此 DES、AES 等针对一维数据流设计的传统加密算法无法应用到图像加密中，我们要设计一种新的加密算法来满足图像加密的要求。混沌系统具有初值敏感性、遍历性、内在随机性等特点，与密码学中的基本要求十分吻合，因此将其应用到图像加密当中具有广阔的前景。

本文对基于超混沌系统的图像加密算法开展了研究，提出了一种基于 Chen 超混沌系统的图像加密算法。在该算法中，首先利用 Arnold 置乱方法来对原始图像进行置乱，改变像素的相关性。然后利用产生的混沌序列对置乱后的图像进行扩散操作得到最终的加密图像。实验结果表明，该算法的密钥空间大，密文像素直方图分布较为均匀，具有不错的加密效果。但应用范围具有一定的局限性，该算法适用于正方形格式的图像。由于系统内的各种参数都是固定的，当攻击者有足够多的样本数据时，会对加密算法进行破解，该算法不能抵御选择明文攻击，以及对差分攻击的抵御能力不强，需要进一步的改进。

在此算法基础上，提出了一种基于 Chen 超混沌系统的明文关联图像加密方案。通过将原始明文图像输入到 SHA-512 函数中得到相应的哈希值，然后计算出混沌系统的初始值和系统参数。在置乱阶段，该方案采用了一种基于混沌序列的置乱方法，使得该方案可以实现任意格式的图像加密。在扩散阶段，方案重新生成了新的混沌系统初始值和系统参数，并且采用异或操作加强明文对密文的敏感性。实验结果表明该方案能抵御选择明文攻击和差分攻击，加密后的像素直方图呈均匀分布，密钥空间大且敏感性强，满足图像加密的基本要求。

关键词： Chen 超混沌系统，SHA-512 函数，明文关联，图像加密

Abstract

With the development of the progress of network information technology, the digital image has become one of the important ways for people to obtain information. Although the digital image has the characteristics of intuitiveness, convenient, and fast, it has gradually gained people's favor, however its security problems can not be ignored. How to ensure the safe transmission of an image through image encryption technology has become one of the hot spots of current research. A digital image has the characteristics of high redundancy, a large amount of data, and strong pixel correlation, which are different from the one-dimensional data stream. Therefore, traditional encryption algorithms designed for the one-dimensional data stream, such as DES and AES, cannot be applied to image encryption. We need to design a new encryption algorithm to meet the requirements of image encryption. A chaotic system has the characteristics of initial value sensitivity, ergodicity, inherent randomness, which is very consistent with the basic requirements of cryptography, so it has a broad prospect in image encryption.

The thesis proposes an image encryption algorithm based on Chen hyperchaotic system. This algorithm utilizes the Arnold scrambling method to scrambling the original image to change the correlation of pixels. Then the chaotic sequence is used to diffuse the scrambled image to get the final encrypted image. Experimental results show that the keyspace of the algorithm is large, the histogram distribution of ciphertext pixels is more uniform, and it has an excellent encryption effect. However, the application scope has some limitations. The algorithm is suitable for square images. Because all parameters in the system are fixed, when the attacker has enough sample data, the encryption algorithm will be cracked. The algorithm can not resist the selective plaintext attack, and the ability to resist the differential attack is not well-built, so it needs further improvement.

Based on the above algorithm, the thesis proposes a Chen-hyperchaotic-system-based plaintext associated image encryption scheme. By inputting the original plaintext image into the SHA-512 function, the corresponding hash value is obtained, and then the initial value and system parameters of the chaotic system are calculated. In the scrambling stage, a scrambling method based on a chaotic sequence is adopted in this scheme, which can realize image encryption of any format. In the diffusion stage, the scheme regenerates the initial value and system parameters of the new chaotic system. It uses exclusive or operation to enhance the sensitivity of plaintext to ciphertext. The experimental results show that the scheme can resist the selective plaintext attack and differential attack. After encryption, the pixel histogram is evenly distributed, the keyspace is large, and the sensitivity is strong, which meets the basic requirements of image encryption.

Keywords: Chen hyperchaotic system, SHA-512 function, plaintext associated, image encryption

目　　录

第 1 章 绪 论

1.1 课题研究背景及意义

随着当前信息化时代的到来，人与人之间、人与物联网之间的信息传递也日益频繁。现如今，互联网技术已经成为人们生活必不可少的一部分，其中发展最快的就是数字多媒体技术，它如今已为我们的日常生活提供了许多便利。相比于传统的文字信息的传播，由于图像信息具有数据量大、传输方便、可解释性强、生动形象等特点，已经成为当前人们交流的主力媒介，然而在人们享受图像传播的便利同时，也存在图像泄露隐私信息等安全隐患。例如一些网络黑客可能窃取含有病人隐私信息的医疗照片，一旦这种隐私照片未经允许得到公开，不仅会损害医院的名誉，同时会对病人造成巨大的伤害。因此研究图像安全信息保密技术变得愈发重要[1-4]。

为了对明文图像信息进行一定的保护，最直观的方法就是对原始明文图像进行加密处理[5][6]。从本质上来讲，对图像进行加密就是将直观明了的明文图像数据转换成混乱无章且无法分辨的密文数据，攻击者不能从加密后的图像中获取有关明文数据的任何信息，因此它需要确定全部的明文数据。对于传统的加密算法来讲，诸如 DES（Data Encryption Standard）算法、AES(Advanced Encryption Standard)算法等传统的加密算法，都是被设计用来加密一维的文本数据，并不适用于二维图像数据的加密。此外，图像数据具有一些固有特点，如像素冗余性强、像素之间信息量大、相关性强等特点，用传统的图像加密算法对图像进行加密时不仅效率低，且加密效果较差，因此需要设计一种加密效果良好、效率较高的图像加密算法。

“混沌”，代表一种混乱无序的状态。随着科学技术的不断进步，混沌理论已逐渐被世界各地的学者所重视。现如今，混沌代表一种发生在确定性关系系统中的不规则的运动，它具有对初始值敏感性、遍历性和伪随机性等特征，例如常被人们所说道的“蝴蝶效应”就是其对初始值敏感性的一种体现。由于混沌系统和传统的密码学之间存在的一些相同点，越来越多的研究人员将混沌系统应用到图像加密中。

在 1989 年 Mattews 首次利用 Logistic 映射生成了一维混沌序列，并将产生的混沌序列用于加密文本消息[7]，虽然该密码系统被应用于文本加密中，并不能用于数字图像加密，但是却证明了混沌系统可以应用到加密领域中，由此许多学者开始把混沌学和信息安全领域相结合，研究出各种加密系统。香农曾提出，一个良好的

加密系统应该包含置乱和扩散两部分[8][9]。其中置乱是指改变像素的空间位置分布来打破原始图像中相邻像素间的强相关性，扩散是指改变像素值的大小，从而改变像素的统计规律。1998 年 Fridrich 提出了一种基于 Baker 映射的图像加密方案[10]，该加密方案中不仅详细的对“置乱-扩散”体系加以描述，并且将混沌映射离散为整数点的一般化方法。从本质上来讲，基于混沌系统的图像加密方案是把明文图像转化为二维矩阵，然后利用产生的混沌序列来对该矩阵进行置乱和扩散操作。随着研究工作的不断开展，更多的混沌加密系统相继被提出，同时部分加密系统还存在一定的安全隐患，因此需要学者更进一步的进行研究，以确保图像加密的安全性。

1.2 国内外研究现状

随着图像信息已逐渐成为互联网时代人们获取信息的主流方式之一，如何去保障信息的安全传输已成为许多专家学者研究的热点之一。传统的加密算法因其固有的特点不适用于图像加密，因此需要研究一种新的加密算法来实现对图像数据的加密。1963 年美国气象学家 Lorenz 发现了混沌运动后，因混沌系统具有良好的伪随机性和密码特性，各国的学者逐渐把混沌系统应用到图像加密中。1998 年 Fridrich 首次提出了一种基于混沌映射的图像加密方法，在该算法中 Fridrich 将混沌系统的迭代值用于实现对明文像素的置乱。然后以此为基础一些学者又设计出了新的加密方案[11][12]。自此以后，有关混沌系统的图像加密算法研究慢慢步入正轨。

一般而言，用于图像加密的混沌系统分为四种：低维混沌系统、多维混沌系统、超混沌系统和复合混沌系统。由于低维混沌系统具有结构简单，便于实现且迭代速度较快等特征，因此被普遍应用于图像加密中[13-15]。文献[16]提出了一种高效的对称图像加密算法，在该算法中利用 Logistic 映射来对图像进行置乱和扩散操作，最终完成对图像的加密。2018 年，文献[17]通过对现有的 Logistic 映射进行改进，把在传统的实数域上的 Logistic 映射推广到有限域当中，并设计了一种彩色图像加密方案，最终实验结果表明该方案不仅效率高，同时加密效果良好。2019 年，程[18]等人通过把三维 Arnold 映射和一维混沌系统相结合，设计了一种控制参数和明文相关联的图像加密方案，极大的提高了加密系统的安全性。文献[19]对当前的一维混沌映射进行改进，提出了一种新的加密算法，改进后的混沌映射密钥空间大，安全性高，整个加密系统的安全性也较高。2020 年文献[20]把 DNA 编码和一维混沌映射相结合，设计了一种新的加密方案，最终实验结果表明该方案的性能比仅仅利用一维混沌映射进行加密的效果要好。随着研究的不断深入，许多学者逐渐意识到低维系统的不安全性。后来经不断研究发现，低维混沌系统有运动学行为简单、参

数较为单一、密钥空间小等问题，因此人们开始对高维的混沌系统进行研究。

相对于低维混沌系统而言，高维混沌系统的运动学行为更为复杂，控制参数更为繁多，系统的随机性更为良好，因此许多学者提出了基于高维混沌系统的加密算法[21-22]。文献[23]中设计了一种基于复合混沌的图像加密方案，改方案利用复合混沌系统来对原始明文图像进行置乱和扩散操作，最终的实验结果表明该算法加密性能良好，安全性高。文献[24]设计了一种基于四维混沌映射和 DNA 系统的图像加密算法，该算法利用四维混沌映射对明文图像进行置乱，用 DNA 规则对像素进行加密以保证图像的安全性。在文献[25]中，设计了一种基于量子 Logistic 混沌映射和复杂超混沌系统的加密算法，该方案具有良好的鲁棒性和高质量的性能，能够切实有效的保护目标图像。文献[26]中提出了一种对称的图像加密方案，该方案中设计了一种新的集成混沌映射来改进低维混沌系统的不足，实验结果表明该方案不仅加密性能优良，同时还能对选择明文攻击有较强的抵御能力。文献[27]设计了一种基于七维混沌系统和哈希函数的加密算法，该方案密钥空间大同时对初始密钥敏感性强，能够抵御多种不同的攻击。

随着人们对混沌图像加密的研究的不断深入，人们通过许多方法来测试密码系统的安全性，如选择明文攻击，差分攻击和统计分析攻击等。为了衡量一个图像加密算法的性能，文献[28]使用了多种指标来评价加密算法的性能，其中最为经典的是像素的改变率(NPCR)和平均一致改变强度(UACI)两个指标，并且一直延续使用至今。而后人们又通过把传统密码学和现代混沌加密相结合，设计了一些良好的加密方案。文献[29]设计了一种基于椭圆曲线密码体制(ECC)的加密算法，通过采用混沌系统和 ECC 两者相结合的方式来加密图像，不仅安全性高，同时便于密钥的管理。直到今天，越来越多的新技术与混沌系统结合在一起，被作用于图像加密中，目前已被成功应用于图像加密中的算法有 DNA 编码[30-32]，压缩感知[33-34]，哈希函数[35-36]等。文献[37]用六维混沌系统生成密钥流，用模运算、异或运算和 DNA 编码技术来对图像进行扩散，该算法安全性高，实用性强。文献[38]将压缩感知应用到图像加密中，并结合随机像素交换算法设计了一种高效的多图像联合加密方案。文献[39]用超混沌系统生成密钥流，其系统参数和混沌系统初始值由明文图像的哈希值产生，由于哈希函数的雪崩效应，不同的图像会产生不同的密钥流，实验结果表明该算法效率高，安全性强。Sun[40]等人设计了一种基于 DNA 编码和超混沌系统的图像加密方法，通过这两者的结合，极大的提升了加密算法的安全性，使得加密算法能抵御各种攻击等。现如今，混沌系统已与许多其他的领域相结合，越来越多的高效、安全的加密算法相继被提出。为了探索出更为高效、安全的图像加密方法，国内外的学者们仍在不断的努力探索中。

1.3 本文研究内容及结构

本文首先论述了课题的研究背景及意义，指出了图像加密的必要性，然后引出了混沌系统，介绍了有关混沌系统的基本知识和基于混沌系统的图像加密的研究现状，在此基础上提出了一种基于Chen超混沌系统的图像加密算法。在该算法中，先用 Arnold 置乱来对原始明文图像进行置乱操作，改变像素的空间分布，然后在扩散阶段，通过对置乱后的图像进行比特移位操作，来改变密文像素间的相关性，完成加密操作。虽然此加密算法加密效果良好，但是不能抵御选择明文攻击，同时对差分攻击的抵御能力不强，因此需要对其作出一定的改进。随着研究工作的不断深入，又提出了一种基于 Chen 超混沌系统的明文关联图像加密方案，该方案把原始明文图像输入到 SHA-512 函数中得到哈希值，然后以此哈希值计算出混沌系统初始值和系统参数，置乱阶段采用了一种基于混沌序列的置乱方法，并且采用比特移位和异或操作对密文进行扩散操作，得到最终的加密图像。实验结果表明，该加密算法密钥空间大，密钥敏感性强，能够抵御选择明文攻击、统计分析攻击和差分攻击，算法安全性高。

本章共五个章节，内容安排如下：

第一章对课题背景和研究意义进行了阐述，介绍了有关混沌系统的图像加密算法的研究现状，概括了本课题的研究内容和章节安排。

第二章介绍了有关混沌图像加密的有关理论，文本加密和图像加密的异同点，混沌系统和密码学之间的关系以及图像加密算法的性能评价指标。

第三章提出了一种基于Chen超混沌系统的图像加密算法，并进行了仿真分析，发现虽然该加密算法效果不错，但是不能抵御选择明文攻击，对差分攻击的抵御能力不强，同时仅仅适用于正方形格式的图片，有一定的局限性。针对以上缺陷，又进行了更为深入的研究，并提出了一种新的图像加密方案。

第四章在第三章的基础了提出了一种基于Chen超混沌系统的明文关联图像加密方案，通过对原始明文图像进行哈希，得到产生的哈希值然后以此哈希值计算出混沌系统初始值和系统参数。然后采用了一种基于混沌序列的置乱方法来改变原始图像的像素的空间分布，通过比特移位和异或操作来扩散置乱后的图像，最终的实验结果表明，该加密算法的密钥空间大，密钥敏感性强，并且能抵御选择明文攻击、统计分析攻击和差分攻击等，算法的安全性较高。

第五章总结了本文的研究工作，并对以后图像加密算法的研究作出了展望。

第 2 章 混沌图像加密相关理论

2.1 混沌理论

混沌是二十世纪以来最重要的发现之一，它代表一种发生在确定性系统中的貌似随机的不规则运动。与伪随机序列的产生类似，只要给予相同的初始条件，就可以对混沌系统的产生进行复现，然而一直以来对于混沌系统并没有一个确定的数学定义。直到 1975 年李-约克在其论文中对混沌系统给出了一个确定的数学定义，自此有关混沌理论的研究慢慢开展开来。随着有关混沌理论的研究深入，人们发现混沌和图像加密之间有许多密切的联系，由此为图像加密的研究带来了新的方向。

2.1.1 混沌的定义

虽然当前混沌存在于各个学科领域当中，但是由于其许多特性并没有被研究透彻，因此至今为止对于混沌并没有一个严谨、完整的定义。现有的一些学者根据自身的研究方向和领域，对混沌作出了一定的解释和定义，目前认可度较高的是 Li-York[41]定义和 Devaney[42]定义，以下将具体介绍这两种定义。

（1）Li-York 定义

1975 年在由李天岩和约克发表的论文“周期 3 意味着混沌”(“Period three implies chaos”)中，对混沌给出了较为准确的定义，即 Li-York 定义：设 f 是定义在闭区间 I 上的连续的自映射，若 f 符合以下条件，则 f 在下述意义下是混沌的：

1）f 的周期点的周期没有上界

2）闭区间 I 存在不可数子集 S 且满足：

i）对任意的 $x, y \in S$，若 $x \neq y$，则有

$$\limsup_{n\to\infty} \left| f^n(x) - f^n(y) \right| > 0 \tag{2.1}$$

ii）对任意的 $x, y \in S$，若 $x \neq y$，则有

$$\liminf_{n\to\infty} \left| f^n(x) - f^n(y) \right| > 0 \tag{2.2}$$

iii）对任意的 $x, y \in S$，其中 y 是 f 的任意周期点，则有

$$\limsup_{n\to\infty} \left| f^n(x) - f^n(y) \right| > 0 \tag{2.3}$$

其中 *sup* 表示上确界，*inf* 表示下确界。

在学术界中，除去 Li-York 定义外，还存在另一个被各国学者广泛使用的混沌定义，即 Devaney 定义。

（2）Devaney 定义

Devaney 定义是从另一个角度，即拓扑理论的角度来对混沌进行阐述的。假设在一度量空间 R 上有一个连续自映射 f，当其满足以下条件时，则称 f 在 R 上是混沌的。

1)拓扑传递性:对于 R 上任意一对开集 $M,N\in R,\exists k>0$，使 $f^k(M)\cap N\neq\varnothing$。

2）初值敏感性：$\exists\delta>0,\forall\varepsilon>0$ 和 $\forall x\in R$，存在 x，y 以及自然数 x，使得在 x 的 ε 领域内满足 $\left|f^n(x)-f^n(y)\right|>\delta$。

3）f 的周期点在 R 处稠密。

2.1.2 混沌系统的基本特征

混沌系统是指在确定性系统中存在的貌似随机的不规则运动，所谓的确定性是指混沌系统的方程是确定不变的，但是该系统的相空间轨迹是类随机的。其中混沌系统具有如下性质。

（1）初值敏感性。对于一个不存在内在随机性的系统而言，当系统中存在较为接近的两个初始值时，则从该初始值出发的系统轨迹是较为接近的。然而对于混沌系统而言，即使是两个非常接近的系统初始值，在混沌系统中经过一定时间的演化后，最终的运动轨迹也大为不同，即为人们常说的“失之毫厘谬以千里”。

（2）系统的内在随机性。它是指在确定性系统中存在的随机性，该随机性是由系统的方程产生而决定的，并且当人们获取了系统的初始值信息后，就可以对原混沌序列进行复现操作。对这种系统的内在随机性存在两种解释，一是因为系统内产生的随机数分布不均匀，另一种是因为混沌系统存在着长期不可预测性。以掷硬币为例，无论我们做多少次掷硬币的实验，都不能根据前一次的掷硬币的结果来推断出下一次掷硬币的结果，混沌系统的内在随机性即是这个道理。

（3）遍历性。遍历性也称为混杂性，在有限时间内混沌轨道能不重复经历混沌吸引子内每一个状态点的领域。

（4）普适性。当系统处于混沌状态的时候，对于不同的混沌系统或者是运动方程存在差异的混沌系统，其混沌状态从外表上来看是相似的。

（5）长期不可预测性。混沌系统由于存在初值敏感性的特征，每对其预测一次，便会丢失一部分信息，多次以后便会丢失较多的信息。因此不能长期预测混沌系统的动力学特性，即混沌系统存在长期不可预测性。

（6）分形性和分维性。所谓分形是指 N 维空间内一个点集的一种几何性质，在任何尺度下都有自相似部分和整体相似性质，具有小于所在空间维数的非整数维数，这种点集叫分形体。分维是用非整数维-分数维来对分形特性的一种定量描述。

（7）有界性。混沌系统的轨迹虽然是杂乱无章的，但并不是无边无际的，最终的运动轨迹会被限制在一定的区域空间内，这个区域空间被称为混沌吸引域。因此无论一个混沌系统的初始值怎么变化，其运动轨迹总是有界限的，这也说明混沌系统总体是稳定的。

2.1.3 混沌系统的判定方法

混沌作为一种非线性动力学系统，被广泛应用于各个学科领域当中。然而并不是每个非线性动力学系统都具有混沌特性。因此如何去判断一个非线性动力学系统是否具有混沌特性，也是混沌学的一个重点研究问题。一般而言，其判定方法有 Lyapunov 指数法，功率谱法，分数维分析法等。以下将介绍几种常用的判断方法。

（1）Lyapunov 指数

Lyapunov（李雅普诺夫）指数常被用于识别混沌运动若干数值的特征之一。在实际当中，假定 Lyapunov 指数为 λ，当 $\lambda>0$ 时，系统运动会进入混沌状态，对应的映射叫混沌映射。当 $\lambda<0$ 时，系统的运动状态会趋于稳定，且此时对系统的初始状态不敏感，即此时的映射对初始值不敏感。当 $\lambda=0$ 时，系统处于稳定状态。

i）一维混沌系统的 Lyapunov 指数计算方法

假定一维系统的运动学方程为 $x_{n+1}=f\left(x_n\right)$，设系统的初始值为 x，此时系统存在一个偏移量 δx，迭代 t 次后可以得到 $\delta x_t=\left|f^{(t)}\left(x+\delta x\right)-f^{(t)}\left(x\right)\right|=\dfrac{df^{(t)}\left(x\right)}{dx}\delta x$，由于系统的运动轨道呈现指数级发散，故用 e^{λ} 表示经过每次迭代后系统运动轨道发散的平均值，其中 λ 表示 Lyapunov 指数，迭代 n 次后可得：

$$\delta x_n=e^{\lambda}\delta x_{n-1}=e^{2\lambda}\delta x_{n-2}\cdots e^{n\lambda}\delta x_0 \tag{2.4}$$

通过求解 λ 可得：

$$\lambda=\frac{1}{n}\ln\frac{\delta x_n}{\delta x_0}=\frac{1}{n}\ln\left|\frac{df^{(n)}\left(x_0\right)}{dx}\right|=\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'\left(x_i\right)\right| \tag{2.5}$$

即最终得到

$$\lambda = \frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(x_i)\right| \tag{2.6}$$

ii）高维混沌系统的 Lyapunov 指数计算方法

设一个 m 维的混沌系统的数学方程如下：

$$\begin{cases} x_{n+1} = f_1(x_n, y_n, \cdots, z_n) \\ y_{n+1} = f_2(x_n, y_n, \cdots, z_n) \\ \cdots\cdots \\ z_{n+1} = f_m(x_n, y_n, \cdots, z_n) \end{cases} \tag{2.7}$$

则该系统的雅克比矩阵为

$$J = \begin{bmatrix} \frac{\partial f_1}{\partial x_n} \frac{\partial f_1}{\partial y_n} \cdots \frac{\partial f_1}{\partial z_n} \\ \frac{\partial f_2}{\partial x_n} \frac{\partial f_2}{\partial y_n} \cdots \frac{\partial f_2}{\partial z_n} \\ \cdots\cdots \\ \frac{\partial f_m}{\partial x_n} \frac{\partial f_m}{\partial y_n} \cdots \frac{\partial f_m}{\partial z_n} \end{bmatrix} \tag{2.8}$$

设系统的初始值为$(x_0, y_0, \cdots, z_0)$，则可求出系统的前$n-1$个雅克比矩阵为：

$$J_0 = J(x_0, y_0, \cdots, z_0), J_1 = J(x_1, y_1, \cdots, z_1), J_{n-1} = J(x_{n-1}, y_{n-1}, \cdots, z_{n-1})$$

设$\lambda_{1i}, \lambda_{2i}, \cdots, \lambda_{mi}\ (i \in [0, n-1])$为各个雅克比矩阵的特征值，$\lambda_1, \lambda_2, \cdots, \lambda_m$为此系统的 Lyapunov 指数，最终求出该系统的 Lyapunov 指数的计算公式如下：

$$\begin{cases} \lambda_1 = \frac{1}{n}\sum_{i=0}^{n=1}\ln\lambda_{1i} \\ \lambda_2 = \frac{1}{n}\sum_{i=0}^{n=1}\ln\lambda_{2i} \\ \cdots\cdots \\ \lambda_m = \frac{1}{n}\sum_{i=0}^{n=1}\ln\lambda_{mi} \end{cases} \tag{2.9}$$

（2）分岔图

分岔一般出现在弹性力学、流体力学和非线性振动的研究中，它表示当系统的参数以微小的状态连续变化时，系统的状态发生明显的改变，即分岔图表示系统随参数变化时由较为稳定的状态进入到混沌状态的过程。

对于一个确定性参数的系统方程来说，若分岔图上只有一个信号点，或者有与系统周期数相同的几个信号点，则说明该系统周期处于稳定的状态。若分岔图上出现无数个随机分布的信号点，并且信号点落在不同的位置上则说明系统处于混沌

的状态。因此分岔图能清晰的刻画出系统的运动状态。

（3）庞加莱(Poincaré)映射

Poincaré 映射是由 Poincaré 在 19 世纪末首次提出，是研究闭轨迹即周期运动的稳定性及其分岔的几何方法，它可以将微分方程描述的非线性系统转化为用差分方程描述的映射。对于空间中的流$\theta\left(x^0;t\right)$，取一个包含x^0而不与$\varphi\left(x^0;t\right)$相切的超平面$\varphi$，可知$x^0$是流$\theta\left(x^0;t\right)$与$\varphi$的第一个交点。沿着流运动，如果存在第一个时间$t_1>0$，使得$\theta\left(x^0;t_1\right)\in\varphi$，那么称$\theta\left(x^0;0\right)$经过一次庞加莱映射到了$\theta\left(x^0;t_1\right)$，记为：$\mathrm{P}\left(\theta\left(x^0;0\right)\right)=\varphi\left(x^0;t_1\right)$。简而言之，庞加莱映射就是初始点从过初始点的超平面开始，沿着流，直到流再次与超平面相交得到一个新的点，即庞加莱映射。

根据 Poincaré 截面，可以用来分析多变量复杂自治系统运动状态。当 Poincaré 截面呈现密集面状时，则系统是超混沌的状态；当截面呈现出密集点状且有层次结构时，则系统是混沌的状态；当截面呈现出封闭曲线时，则系统处于圆环面或准周期状态；当截面呈现出少数的离散点时，则系统处于周期状态。

（4）测度熵

熵在信息论中是最常用的参数之一，它是用来描述信源的不确定度。由于混沌系统的局部不稳定性，使得其相空间中的相邻轨道以指数速率分离。当系统中的两个初始点以这种方式相互靠近时，在随后的一段时间内不能通过测量的方法来区分这两条轨道，在其充分分离后才能对其进行区分。在此意义上，混沌运动产生的信息量与可区分的不同的轨道数目 N 有关，其中 N 随时间指数增长

$$N \propto e^{(Kt)} \tag{2.10}$$

常数 K 刻划信息产生的速率，即测度熵。对于确定性系统的规则运动，测度熵的值为 0；若测度熵的值趋近于无穷，则该系统为随机性系统；混沌系统的测度熵的值为大于 0 的常数，测度熵的值越大，则信息的损失速率越大，系统的混沌程度越大。

（5）功率谱分析

对于混沌系统而言，功率谱分析是用来研究其混沌行为，揭示其系统内部的随机性。从本质上来说，功率谱分析是通过将时间空间转化为频率空间来阐明时间信号的频率结构。对于周期性运动而言，功率谱仅在基频和其倍频会出现峰值。对于混沌系统而言，虽然功率谱也会存在尖峰，但其会增宽一些，并且不再与相应采样频率变化，并且在功率谱上会有很宽的噪声背景。因此通过功率谱来确定系统的准周期和混沌是非常有效的。

2.1.4 几种典型的混沌系统

混沌系统发展至今，有着许多的性能优良的混沌系统，下面将介绍几种典型的混沌系统。

（1）一维 Logistic 映射[43]

Logistic 映射亦被人们称为虫口模型，是一个常见的非线性迭代方程，其定义如下：

$$x(n+1)=Rx(n)(1-x(n)) \tag{2.11}$$

当 Logistic 混沌映射初始值 $x(0)\in(0,1)$，控制参数 $R\in(3.5699\ldots,4]$ 时，系统随着控制参数 R 的微小增加而不断进行周期分岔，然后逐步通向混沌状态。从图 2.1 可以看到 Logistic 混沌系统根据参数 R 的不同由倍分岔进入到混沌状态的过程。

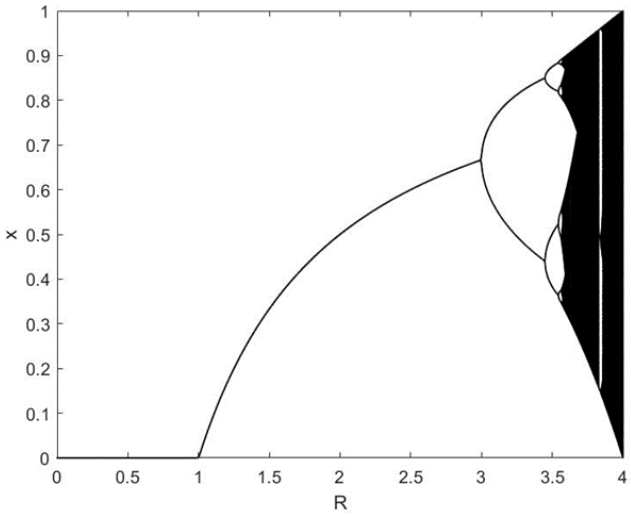


图 2.1 Logistic 映射分岔图

（2）二维 Henon 映射[44]

1976 年 Henon 提出了一种二维映射被称为 Henon 映射，其定义如下：

$$\begin{cases} x_{n+1}=1+y_n-ax_n^2 \\ y_{n+1}=by_n \end{cases} \tag{2.12}$$

其中参数 $a\in(0,1.4]$，$b\in(0.2,0.314]$。当 $a\in(0,1.4)$，$b=0.3$ 时，该系统分岔图如图 2.2 所示，当 $a=1.4$，$b=0.3$ 时，系统处于混沌状态，该系统吸引子如图 2.3 所示。

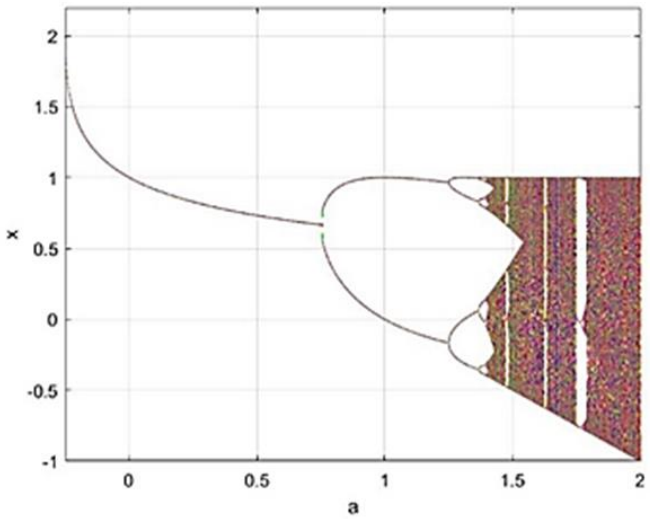


图 2.2 Henon 映射分岔图

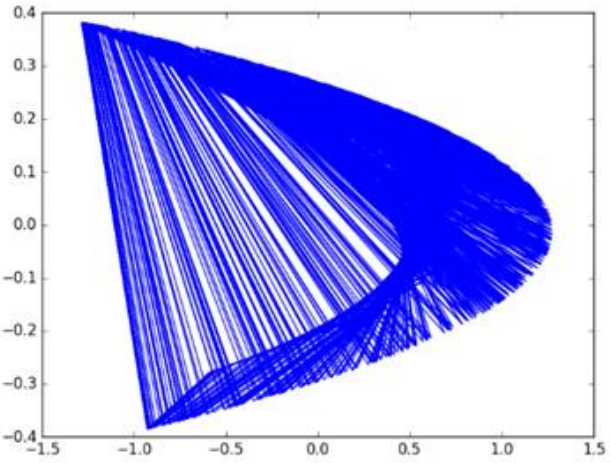


图 2.3 Henon 映射吸引子

（3）三维 Lorenz 混沌系统[45]

1963 年，Lorenz 提出了一种三维混沌系统，其运动状态方程组为：

$$\begin{cases} \dot{x} = -a(x-y) \\ \dot{y} = cx - xz - y \\ \dot{z} = xy - bz \end{cases} \tag{2.13}$$

其中 a,b,c 为系统控制参数，当其取值分别为 10、8/3、28 时，混沌系统吸引子如图 2.4 所示。

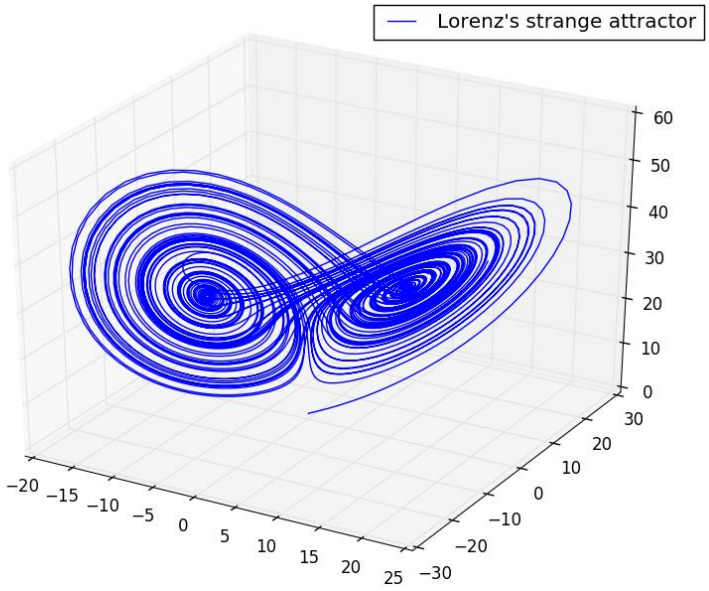


图 2.4 Lorenz 映射吸引子

2.2 密码学基础

2.2.1 密码学基本概念

密码学是一门研究编制密码和破译密码的技术科学。现阶段，随着时代的进步和社会的发展，密码学已逐渐扩散到民用领域，成为我们日常生活中的一部分。如云上面隐私信息的加密，软件的源代码的保密等。对于一个完整的密码通信系统而言（如图 2.5 所示），它由五个部分组成：明文，密文，密钥，加密算法，解密算法。其具体含义如下：

图 2.5 密码系统

明文：未进行加密，直接代表原文含义的消息。

密文：已加密的信息，一般而言，外在用户不能从密文中获取有关明文相关的信息了。

密钥：在加解密的过程中，需要借助一些具体的参数来完成这整个过程，这个参数叫做密钥。

加密算法：将明文转变成密文的实施过程。

解密算法：将密文转变成明文的实施过程。

2.2.2 安全性和密码分析

一个完美的密码算法的设计离不开密码分析，所谓密码分析，是指研究在通常情况下不知道解密所需的秘密信息，对信息进行解密的学问。一个好的加密算法，需要抵抗各种各样的攻击，在实际应用中，人们通过不断总结和优化，研究出了一些密码分析和攻击的手段，下面将介绍几种常见的攻击分析方法：

（1）穷举分析攻击。

穷举攻击也被称为暴力破解，即攻击者列举出所有可能的密码，用这些数据一一尝试，从而达到破解的目的。但是这种破解方法需要精密的设备、足够大的计算空间和存储空间等条件。从理论上来说，这种破解方法能够破解任何密码系统，包括“一次一密”密码系统，但是在实际操作中，受到时间和人力等资源条件的限制，导致穷举分析攻击的可行度较低，比如当用计算机对一个密码系统的密钥空间进行破解时，可能计算时间开销需要几十年，这样导致用穷举分析攻击方法失去了意义。因此在密码系统中，一般可通过增大密钥空间的方法来抵御穷举攻击。

（2）统计分析攻击。

一般来讲，密码系统的密文和明文之间会存在一定的统计规律，所谓统计分析攻击，是指密码分析者根据密码系统中的明文、密文和密钥之间存在的统计规律来对系统进行破译的一种方法。例如，在原先的经典的置换密码和换位密码体制中，可通过分析单字母、双字母等的频率和其他统计参数而破译。对抗统计分析攻击的主要方法是消除密文间的统计特性。这样密文之间没有明文的统计规律，会呈现出一定的随机性，从而能抵御统计分析攻击。

（3）数学分析攻击。

数学分析攻击，是指密码分析人员针对加密算法或解密算法中存在的数学规律、密码学特性，通过一系列数学求解来进行破译的方法。为了抵御数学分析攻击，应当选用结构较为复杂的算法来完成对明文信息的加密。

除去以上这些攻击外，还存在其它的攻击方式。根据 Kerckhoffs 准则，一个良好的密码系统的安全性不应取决于算法本身的保密，而应该取决于它的密钥对于攻击者来说是保密的。当攻击者拥有足够多的有关密码系统的信息时，则可能会对密钥进行破译。根据攻击者手中掌握的资源情况的不同，密码分析一般可分为以下几种攻击分析方式：

（1）唯密文攻击。

唯密文攻击是指攻击者在仅知密文信息的情况下进行攻击。

（2）已知明文攻击。

已知明文攻击是指密码分析者知道一些特定的明文和其对应的密文，然后推导出加密的密钥或算法。

（3）选择明文攻击。

攻击者不仅知道加密的算法，还可以选定明文消息并得到与其对应的密文，然后对密钥进行破译。

（4）选择密文攻击。

攻击者可自行选择密文并得到其对应的明文消息，通过对这些“密文-明文”进行分析，最终破译出密钥。

对于一个良好的加密系统而言，必须能抵抗各种各样的攻击，才能保证加密信息的安全性。

2.2.3 混沌系统和密码学的联系

混沌系统和密码学的结合，给图像加密带来了新的研究方向，即基于混沌的图像加密技术，其本质是利用混沌系统产生的序列，对图像数据进行加密，并取得了良好的效果。下表 2.1 给出了混沌系统和密码学之间存在的异同点。

表 2.1 混沌与密码学的异同点

对比	混沌理论	密码学
相同点	对系统参数和初始值敏感	扩散
	伪随机性和不稳定性	伪随机性
	系统参数	加密密钥
	将初始值扩散到整个相空间	多轮加密实现置乱和扩散
不同点	定义域为实数域	加密算法定义在有限集
	缺少理论分析	完备的安全性分析

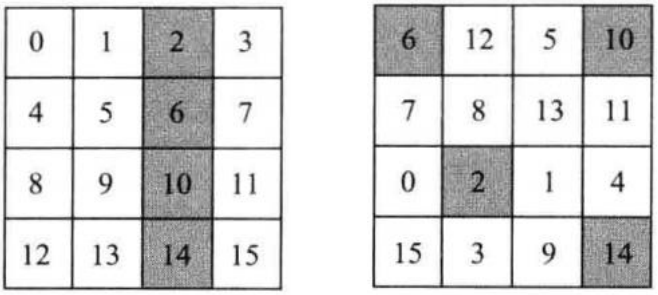
从上表中可以看出，混沌理论和密码学有一些相同点和不同点，这些相同点说明将混沌理论应用在密码学领域中是可行的，同时混沌理论可以和密码学之间相互借鉴；另一方面，这些不同点为以后把混沌理论和密码学的融合提供了研究方向。

2.2.4 图像加密技术

近年来随着互联网和多媒体技术的迅猛发展，如何确保信息的安全传输已经成为当前研究的热点。在日常生活中，由于图像信息具有生动形象、渲染力强和信息量大等特点，因此被广泛传播。为了保证图像信息的安全传输，需要对其进行加密处理。而传统的加密算法都是针对一维的数据流而设计，不适用于图像加密，因此需要一种新的加密方法来加密图像。在计算机中，数字图像是以像素值矩阵的形

式而存在的，因此可以将像素矩阵转变成一维的数据流形式，再将像素的原始位置进行打乱或者对其进行加密处理，最后再转变成矩阵的形式，从而得到最终的密文图像。图像加密可以按照不同的方式进行分类，当把图像加密按照加密时像素位置和像素灰度值是否改变来区分时，将仅改变位置的加密称为置乱加密，而将仅改变明文像素灰度值大小的加密称为灰度加密。若两者都有改变，则称为混合加密。目前，许多学者都曾提出过有关图像加密的算法，以下将介绍几种传统的图像加密算法。

（1）图像置乱加密算法：图像置乱加密即将明文图像的像素在空间上进行重新排列，简称重排，通过置乱操作可以让原始明文图像变成无意义的混乱图像。以下图为例，一幅 4×4 的图像，如图 ，通过某种置乱算法实现了像素的重排，如图 2.6 所示。



（a）原始图像　　（b）置乱图像

图 2.6 图像的置乱

图像的置乱加密仅仅改变了像素的空间位置，并不会改变像素值的大小，常见的置乱变换有 Arnold 变换、幻方变换、Hilbert 曲线变换等。由于其像素值大小没有改变，因此像素间仍然存在一定的统计规律，攻击者可以通过直方图分析来对置乱加密算法进行破解。

（2）图像扩散加密算法：图像扩散加密是指改变原始图像的灰度值来对图像进行加密，与图像的置乱加密相对应，图像的扩散改变了像素值的大小，因此密文图像的直方图也会发生变化，攻击者很难通过直方图分析来破解加密算法。文献[46]中介绍了一种基于像素值替代的加密算法，在该算法中将明文图像分割成若干个大小不一的块，块的大小是表 2.2 中的任意一个。

表 2.2 每一轮中块的大小

Mod10	0	1	2	3	4	5	6	7	8	9
块大小	16	24	32	40	48	56	64	72	80	96

为了形成相邻像素对，在第一轮迭代中，所有的子密钥和方块都作为像素的起始位置，该方法使得攻击者无法得到用于特定方块的子密钥对，因此提高了加密算

法的安全性。

（3）混合加密：混沌加密即指图像置乱-扩散算法。在传统的加密算法中，图像的置乱加密仅仅改变了像素的位置，并没有改变像素值的大小；而图像的扩散加密仅仅改变了像素值的大小而没有改变像素的位置，因此其安全性都不高。考虑到图像的本身的特点，现如今图像的置乱-扩散加密算法已经成为主流。在这种加密体制下，加密后的像素值的大小不仅取决于像素的初始位置，还取决于其周围像素的灰度值的大小。实验证明该加密算法的安全性比传统的置乱、扩散加密算法效果要好。

2.2.5 图像加密特点

混沌系统和密码技术的结合，诞生了基于混沌系统的图像加密技术。与文本信息不同，在对原始图片进行加密的过程中，明文图像是一个二维数组，像素之间具有较高的冗余度和相关性。此外，图像加密还应能保证实时加/解密等。以下为图像加密和文本加密的区别。

1. 当对文本进行加密时，加密后产生的密文必须完全无损，同时解密后得到的文本必须完全等于原明文，不能有丝毫的差别。然而在对图像进行加密时，加密图像可允许部分损失解密成原图像。
2. 文本数据在电脑中是二维的数据流，因此可以直接用分块或密钥流加密。而数字图像在计算机中具体表现为二维矩阵，不能进行直接加密。
3. 与文本消息相比，图像的存储空间较大，若对图像文件直接进行加密/解密，效率较低。为减少其存储空间和传输时间，方法之一是加密/解密其被压缩的信息部分。

一个完善的加密体系不仅要保证良好的安全性，同时还要能高效的运行。对于图像加密而言，系统安全性应具备以下特征：

1. 加密系统在计算上是安全的，在有限特定时间内对算法破解是不可行的，同时未授权用户不能读出特定的图像。
2. 图像必须能保证实时加/解密，能满足个人用户的日常使用。
3. 安全机制应当是柔韧的。
4. 加密后的图像数据不能发生较大的密文膨胀。

2.2.6 图像加密算法评价标准

一个良好的图像加密算法需要有能够抵御各种各样的攻击的能力。在加密算法实现后，需要对算法进行评估和分析，以确定该算法是否安全可靠。一般而言，

评价一个图像加密算法的性能，需要进行以下几种分析。

灰度直方图：Shannon 提出许多对于种类的加密方法，用统计分析方法是可能解密的。在灰度直方图中，它能够清晰的反映出每个不同的灰度值下的个数以及整体的灰度级的分布。当加密后的图像的灰度直方图分布愈趋于平滑，则说明加密算法的性能越好。

信息熵：图像的信息熵可以度量灰度值的分布，当图像中各个灰度值出现的概率相等时，图像的信息熵最大。根据 Shannon 定理，图像的信息熵为

$$H(m)=-\sum_{i=0}^{L-1}p(m_i)\log_2 p(m_i),\sum_{i-0}^{L-1}p(m_i)=1 \tag{2.14}$$

其中 H 为图像的信息熵，L 为图像像素特征的总个数，$p(m_i)$ 为各个灰度值出现的概率。

相邻像素相关性：相关性是指两个变量的关联程度。在图像加密领域中，它是指相邻两像素之间的相关性，包括水平、垂直和对角线三个方向。其计算公式如下：

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2.15}$$

$$\begin{cases} E(x)=\dfrac{1}{N}\sum_{i=1}^{N}x_i \\ D(x)=\dfrac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2 \\ \operatorname{cov}(x,y)=\dfrac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)\left(y_i-E(y)\right) \end{cases} \tag{2.16}$$

其中 x 和 y 表示为图像中两个相邻像素的灰度值。

明文敏感性：在实际应用中，差分攻击是一种常见的破解加密系统的方法。所谓差分攻击，是指攻击者对原始图像作出微小的改变，并用加密算法对修改后的图像进行加密，得到加密后的图片，然后通过比较两幅加密后的图像，寻找原始图像和加密后的图像的联系。对于图像加密而言，为测试一个像素改变后的影响，一般采用两种测量方法：像素改变率(number of pixels change rate，NPCR)和一致平均改变强度(unified average changing intensity，UACI)，其定义如下：

$$NPCR=\frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}D(i,j)\times 100\% \tag{2.17}$$

$$UACI=\frac{1}{M\times N\times 255}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left|C_1(i,j)-C_2(i,j)\right|\times 100\% \tag{2.18}$$

其中 M 和 N 表示图像 C_1 和 C_2 的宽度和高度，$C_1(i,j)$ 和 $C_2(i,j)$ 表示两幅明文图像仅有一个位置的像素差值，且差值为 1。对于一个灰度值图像而言，NPCR 和

UACI 的理想值为 99.6094%和 33.4635%。

密钥空间分析：一个优良的加密算法对于密钥应是敏感的，其密钥空间应该足够大并能抵御各种攻击。密钥空间分析包括加密密钥数量分析和密钥灵敏度测试，其中加密密钥数量分析是用来衡量加密算法的密钥能否抵御穷举攻击，密钥灵敏度测试要求只有加密密钥和解密密钥完全一致时，才能正确解密出明文图像。

第三章 基于 Chen 超混沌系统的图像加密算法

近年来，涌现了许多基于各种变换的加密算法，如幻方变换、骑士巡游等。在这些置乱算法中，都是基于某种数学规律来改变原始图像的像素位置，从而实现对原始图像的置乱加密。但是仅仅对原始图像进行置乱加密安全性较低，攻击者可以通过一些不同的方式来实现对密文图像的破解，因此将置乱和扩散相结合的加密方式才能对图像进行更好的加密。在本章中提出了一种基于 Chen 超混沌系统的图像加密算法，该算法利用“置乱-扩散”体系来对图像进行加密，最后对算法的性能进行仿真实验。

3.1 基于 Chen 超混沌系统的图像加密算法

在本算法中，先用 Arnold 置乱来对原始图像进行置乱得到行列置乱图像。然后设定初始值得到产生的混沌序列，从混沌序列中截取部分混沌序列来对置乱图像进行扩散，从而改变像素值。算法流程如图 3.1 所示：

图 3.1 算法流程图

3.1.1 Chen 超混沌系统

自 1963 年首个混沌系统被发现后，更多的混沌系统也不断被发现。其中 Chen 超混沌系统具有更复杂的拓扑结果和动力学行为，其方程如下：

$$\begin{cases} \dot{y}1 = a\left(x_2 - x_1\right) + x_4 \\ \dot{y}2 = bx_1 - x_1x_3 + cx_2 \\ \dot{y}3 = x_1x_2 - dx_3 \\ \dot{y}4 = x_2x_3 + ex_4 \end{cases} \tag{3.1}$$

其中 a,b,c,d,e 是控制参数，当参数取值 $a=35,b=7,c=12,d=3,e=0.797$ 时，系统处于超混沌状态。在本文中采用四阶 Runge-Kutta 算法对 Chen 超混沌系统进行离散化处理，取迭代步长 $h=0.001$，起初始值为 0，终止值为 80，MATLAB 仿真得到 Chen 超混沌系统相图如图 3.2 所示：

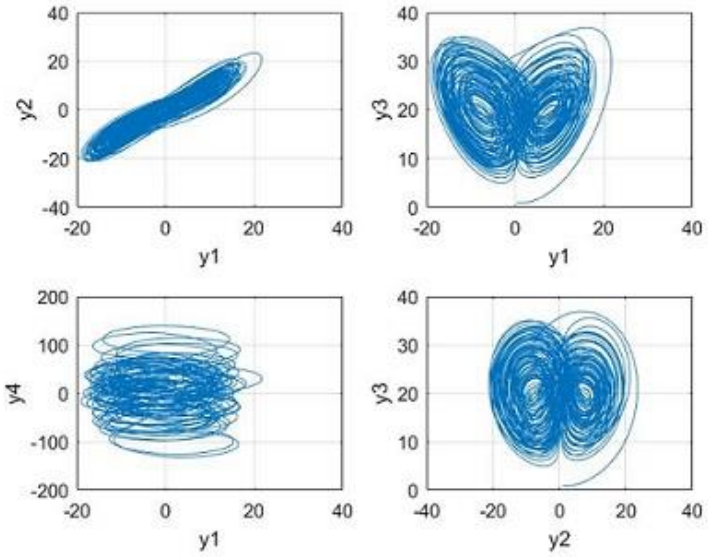


图 3.2 Chen 超混沌系统相图

3.1.2 图像行列置乱

图像的行列置乱是指改变原始明文像素的空间分布，降低像素之间的空间相关性，最终达到隐藏明文图像信息的目的。Arnold 置乱因其具有效率高，操作简单等特点而被应用于图像加密当中，该置乱方法的本质是拉伸和延伸。传统的 Arnold 置乱矩阵形式可表示为：

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N \tag{3.2}$$

假设原始输入图片格式为 $N \times N$，(x, y)代表原始图像的像素位置。Arnold 置乱具有周期性，即经过若干次数的置乱后，置乱图像又恢复成了原始图像。

3.1.3 混沌序列生成

在本章节中，用 Chen 超混沌系统来产生混沌序列，最终可得到 4 个混沌序列。在得到产生的混沌序列后，为了加强序列的伪随机性和避免暂态效应，要对产生的混沌序列进行优化处理，即截取序列的部分长度来对图像进行扩散处理，最终得到密文图像。

假设原始明文图像格式为 $N \times N$，即有 $N \times N$ 个像素点。首先，设定混沌系统初始值为 (x_1, x_2, x_3, x_4)，代入到混沌系统方程中进行迭代得到四组混沌序列串 (x_1', x_2', x_3', x_4')，舍弃序列的前 T 个序列，然后截取新的长度为 $N \times N$ 的混沌序列串 $X = (X_1, X_2, X_3, X_4)$，对序列 X 按照公式进行改造：

$$R_i(r)=\left(\left(abs\left(X_i(r)\right)\times 10^{10}\right)\bmod 7\right)+1 \tag{3.3}$$

$$R_j(r)=\left(abs\left(X_i(r)\right)\times 10^{10}\right)\bmod 256 \tag{3.4}$$

其中 *abs* 函数表示取绝对值，*mod* 函数表示取余，最终得到的混沌序列 R_i 的取值范围在[1, 7]之间， R_j 的取值范围在[0, 255]。

3.1.4 图像像素扩散

图像的行列置乱操作仅仅是改变了明文图像像素的空间相关性，并没有改变像素之间的统计规律，导致加密后的图像的安全性较低。为了提升图片的加密效果，在对图像进行置乱操作后，再对其进行扩散操作。在本算法中，先把 $N\times N$ 格式的原始图片按照行优先的原则转变成一维序列 $L=\left[l(1),l(2),\ldots,l\left(N\times N\right)\right]$，按照公式进行扩散操作，公式如下：

$$C(r)=circshift\left[L(r),LSB\left(R_i'(r)\right),R_i(r)\right] \tag{3.5}$$

$$C'(r)=C(r)\oplus R_j(r) \tag{3.6}$$

上述公式中，$circshift[u,q,v]$表示对序列 *u* 进行 *v* 比特的循环移位操作，当 $q=0$ 时对其进行向左的循环移位，当 $q=1$ 时对其进行向右的循环移位。*LSB* 函数表示二进制数字的最低有效位。 R_i' 为序列 R_i 的二进制表示， $\oplus$ 表示异或操作。

3.1.5 加解密过程

具体加密过程如下：

算法：基于 Chen 超混沌系统的图像加密算法

输入：原图像

输出：加密图像

Step 1：将混沌系统初始值代入到混沌系统中进行迭代，得到四组混沌序列；

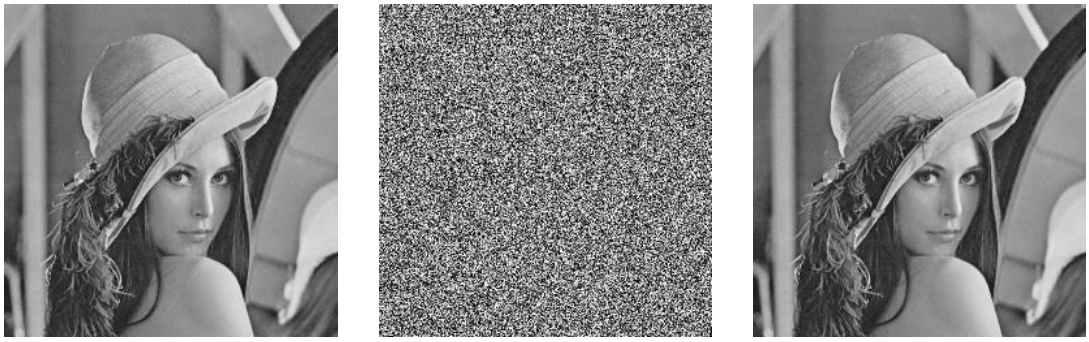
Step 2：选取其中一组混沌序列，并截取部分混沌序列并对序列进行改造，按照方法 得到新的序列 R_i；

Step 3：按照公式(3.2)对原始图像进行置乱若干次，得到新的置乱图像后再将其转化为一维序列 L；

Step 4：按照公式(3.5)对序列 L 进行移位扩散操作，并按照公式(3.6)与改造后的混沌序列 R_j 进行异或操作，完成对像素的扩散操作；

Step 5：将扩散后的一维序列重新整合为$N \times N$的图像矩阵，输出最终的密文图像。

解密过程为加密过程的逆操作，先将密文图像整合成一维矩阵，然后对矩阵中的元素进行异或操作和反向移位，此时需要知道产生的混沌序列值，最终将完成扩散解密的矩阵还原成$N \times N$的图像矩阵，并对该图像矩阵进行若干次数的置乱，还原出原始明文图像。本算法采用 Lena 灰度图像进行加解密操作，效果如下：



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

图 3.3 Lena 加解密图像

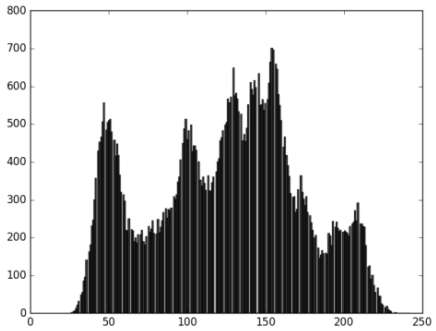
3.2 实验结果分析

3.2.1 密钥空间分析

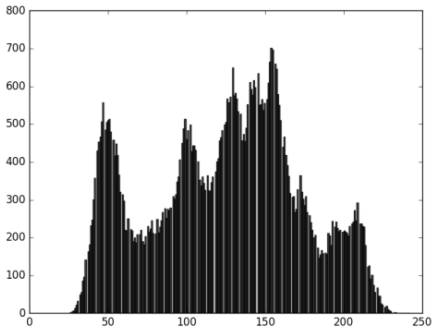
本算法的密钥空间主要有以下几部分组成：Chen 超混沌系统的初始值，在对原始图片进行 Arnold 置乱时的置乱次数，以及选择混沌序列时的系统控制参数。计算机的精度为10^{-15}，根据密钥初始值计算密钥空间为$10^{15} \times 10^{15} \times 10^{15} \times 10^{15} = 10^{60}$，密钥空间足够大能够有效抵御暴力破解，如果考虑到明文图像的置乱次数和系统的控制参数，则密钥空间更大，更能抵御来自敌手的暴力破解。

3.2.2 直方图分析

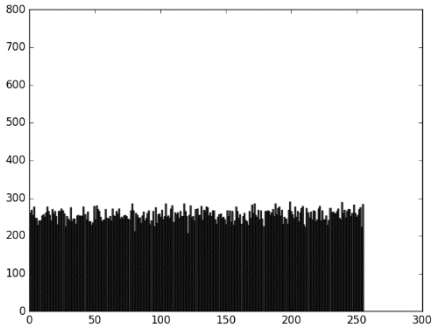
图像的灰度直方图能够反应每个像素点的统计规律，一般而言明文图像的灰度值分布会有向某些灰度值集中的趋势，因此这部分像素灰度值容易遭到攻击者的统计分析。对于理想的图像而言，像素的灰度值分布直方图愈趋于平滑，则攻击者通过统计分析来获取像素的有关信息的难度就愈大，图 3.4 表示原始 Lena 明文图像的直方图、置乱后的 Lena 直方图和加密后的 Lena 直方图，从图 3.4 中可以看出，原始 Lena 明文像素之间存在明显的统计规律，在对 Lena 图像进行置乱后，并没有改变像素之间的统计规律，最终得到的加密后的图像直方图发生了明显的改变，像素直方图比较均已平滑，说明加密后的图像能够抵御攻击者的统计分析。



(a) 原始 Lena 图像直方图



（b）置乱后 Lena 图像直方图

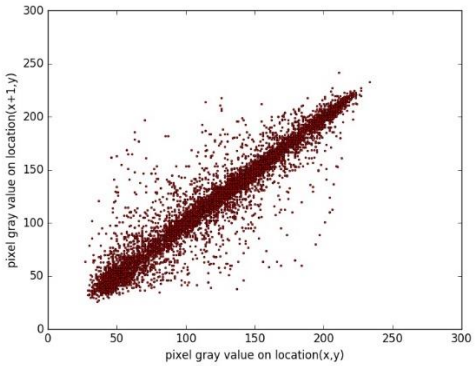


(c) 密文图像直方图

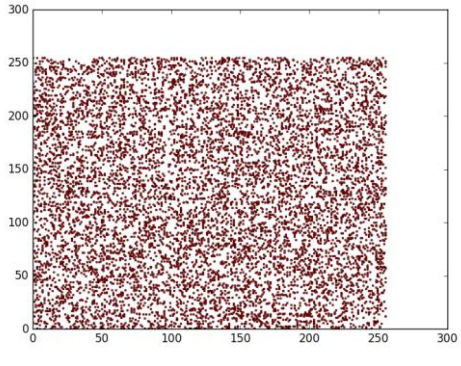
图 3.4 统计直方图

3.2.3 相邻像素相关性分析

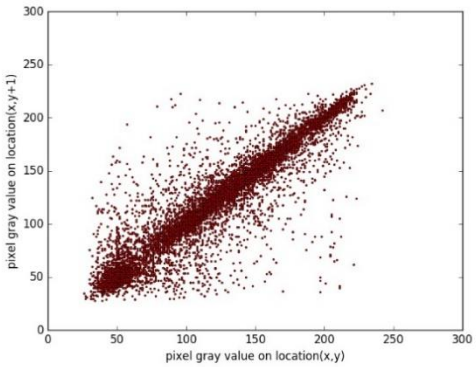
对于明文图像而言，像素之间相关性强，它的某个像素的灰度值和与周围像素的灰度值非常接近，因此易遭到攻击者的破解。对于一个良好的密文图像而言，其像素之间相关性越弱，则该加密方案安全性越高。在本方案中，随机选取 Lena 明文图像和密文图像水平、垂直、对角三个方向相邻像素进行相关性分析，表 3.1 不仅表示了原始明文 Lena 图像与其密文图像像素之间的相邻系数，还与其它方案进行了对比。从表 3.1 中可以看出，加密后的像素相关性有了明显的降低，但与别的加密方案比较，本方案的加密相关性效果不是很好。图 3.5 表示原始图像和加密后图像像素的散点图。



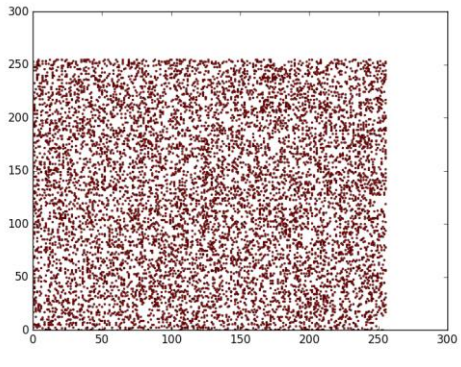
(a)明文水平方向



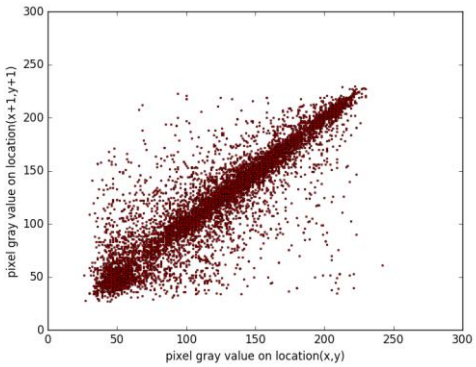
(b)密文水平方向



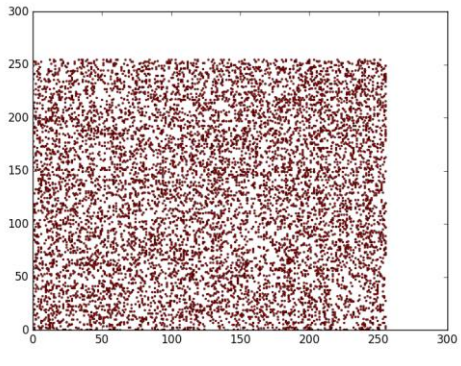
(c) 明文垂直方向



(d)密文垂直方向



(e) 明文对角方向



(f)密文对角方向

图 3.5 相邻像素点的相关性分析

表 3.1 不同加密方案加密 Lena 的相关系数

算法	水平方向	垂直方向	对角方向
明文图像	0.956	0.916	0.901
本方案	0.0252	0.0197	0.0493
[47]	0.0272	-0.0114	-0.0484
[48]	0.0214	0.0465	-0.009

3.2.4 信息熵分析

信息熵是用来衡量加密后的密文图像像素是否是伪随机分布的一个指标，由信息熵公式可知，其值越大，表明像素的随机性分布越好。对于一个灰度值图像来讲，加密后图像的理想熵值为$\log_2 256$，即值为 8。因此当加密后的图像信息熵的值愈趋近于 8，则说明加密的效果越好。在本算法中，加密后的 Lena 图片信息熵为 7.9601，比较接近理想值 8，表明密文图像像素点随机分布。

3.2.5 差分攻击分析

差分攻击是指攻击者对两张具有微小差别的明文图像用相同的加密算法来进行加密，然后比较密文图像之间的差异，从中发现规律来破解加密密钥的手段。在图像加密中，像素改变率(NPCR)和平均一直改变强度(UACI)是用来衡量加密算法抵御差分攻击能力的重要指标，NPCR 和 UACI 的理想值分别为 99.6094%和 33.4635%，当加密后的密文图像的 NPCR 和 UACI 值愈接近理想值，则表明该算法抵御差分攻击的能力越强。在本算法中，计算 Lena 密文图像的 NPCR 和 UACI 值，并与文献[49][50]作对比，结果如表 3.2 所示。从表中可知，加密后的图像的 NPCR 和 UACI 值比较接近理想值，能够有效的抵御差分攻击。

表 3.2 测试图像的 UACI 和 NPCR 值

方案	UACI 值	NPCR 值
本算法	32.852%	98.332%
[49]	28.27%	99.54%
[48]	33.44%	99.58%

3.3 本章总结

本章设计了一种基于 Chen 超混沌系统的图像加密算法，首先利用 Arnold 置乱对原始明文图像进行置乱，再结合产生的混沌序列来对置乱后的图像进行扩散操作，进而改变明文像素的统计规律。在进一步的实验仿真分析中表明，该算法具有密钥空间大，加密后的像素随机性较好等优点，满足图像加密的基本要求。

第四章 基于 Chen 超混沌系统的明文关联加密方案

在上一章中提出了一种基于 Chen 超混沌系统的图像加密方案，该方案虽然能满足图像加密的基本要求，但也存在一些问题和不足。比如在对原始明文图像的置乱过程中，采用的是传统的 Arnold 置乱的方法，该置乱方法虽然操作简单、方便快捷，但是仅仅使用于 $N \times N$ 格式的图像，具有一定的局限性。另外在该算法中，系统的各种控制参数都是固定的，当攻击者拥有足够多的样本时，会分析破解出系统参数值，存在一定的安全隐患。在本章中提出了一种基于 Chen 超混沌系统的明文关联加密方案，首先利用 SHA-512 函数获得原始明文图像的哈希值，然后根据产生的哈希值依照特定的公式来计算混沌系统的初始值和系统内部控制参数。由于哈希函数自身的固有特性，对于不同的明文图像一定会产生不同的哈希值，因此对于不同的图像哈希值计算出的混沌系统初始值和系统参数一定不同，所以该算法有较强的抵御选择明文攻击的能力。在置乱阶段，采用了一种新的基于混沌序列的置乱方式，该置乱方式适用于 $M \times N$ 格式的图片。在扩散阶段，系统内的各种参数都是根据置乱阶段的参数哈希值计算出来的，并且在最终扩散阶段，密文像素值前后相联系，敏感性强，最终完成了对原始明文图像的加密。

4.1 SHA-512 函数简介

安全哈希函数是(SHA)是使用最广泛的 Hash 函数，1993 年美国标准与技术研究所(NIST)设计并发表了哈希函数，该版本的哈希函数被称为 SHA-0，由于发现该哈希函数存在一定的安全隐患，于是在 1995 年发布了 SHA-1。随着时代的发展，SHA-256、SHA-384、SHA-512 也陆续被发布，这些算法被统称为 SHA-2。一直到现在为止，SHA-2 各版本已经成为主流。哈希函数之所以能被应用于信息安全领域当中，是因为其具有以下特点：

- 压缩性：对于任意长度的明文输入，算出的摘要长度都是固定的。
- 抗修改性：对于两个不同的明文输入，哪怕仅仅只有 1 比特的不同，其输出也是不同的。
- 强抗碰撞性：要找到两个不同的数据，使它们具有相同的输出，在计算上是困难的。
- 若抗碰撞性：已知原始数据和其输出摘要，要找到一个具有相同输出摘要的数据（即伪造数据），在计算上是困难的。

基于以上特征，SHA-512 函数基本实现流程如下：

步骤 1：补充附加位。

当一副明文图像被作为明文输入到 SHA-512 函数中，首先图像中的每一个像素会被转化成二进制编码形式，即整个图像被转化成一个二进制字符串。对于 SHA-512 算法来讲，其输入必须满足以下条件，长度对 1024 取模的余数为 896。即使原始输入满足该条件，也要进行补位，补位是由一个 1 和后续的 0 组成，直到满足条件。

步骤 2：补充长度位。

在补充附加位后，字符串中已经没有字符串的长度信息，因此需要补充长度位。在填充的消息后附加 128 位的块，将其视为无符号整数，并且包含前消息的长度。在补充完长度位后，产生了一个长度为 1024 整数倍的消息，以便进行后续的分组。

步骤 3：初始化哈希缓冲区。

Hash 函数中间结果和最终结果保存在 512 位的缓冲区，缓冲区由 8 个 64 位的寄存器(a,b,c,d,e,f,g,h)表示，并将这些寄存器初始化为下列 64 位的整数（十六进制）：

a = 6A09E667F3BCC908　　e = 510E527FADE682D1

b = BB67AE8584CAA73B　　f = 9B05688C2B3E6C1F

c = 3C6EF372FE94F82B　　g = 1F83D9ABFB41BD6B

d = A54FF53A5F1D36F1　　h = 5BE0CD19137E2179

每个寄存器内容获取的方式是：取前 8 个素数（2、3、5、7、11、13、17、19）取平方根，取小数部分的前 64 位。

步骤 4：计算哈希值。

以 1024 位分组为单位处理消息，最后输出结果得到最终的哈希值。

4.2 基于 Chen 超混沌系统的明文关联加密方案

在本算法中，先利用 SHA-512 函数对原始明文图像进行哈希操作，得到 512 位的二进制哈希值，然后根据此哈希值计算出混沌系统的初始值和一些系统控制参数，再把混沌系统初始值代入到 Chen 超混沌系统中进行迭代，得到混沌序列值，此时根据混沌序列值和部分系统参数来对原始明文图像进行置乱，得到置乱后的图像。再把置乱后的图像作为 SHA-512 函数的输入，得到新的 512 位的二进制哈希值，然后再计算出新的一轮的混沌系统初始值和系统控制参数，再对置乱后的图像进行扩散操作，最终得到加密后的密文图像，算法流程图如图 4.1 所示。

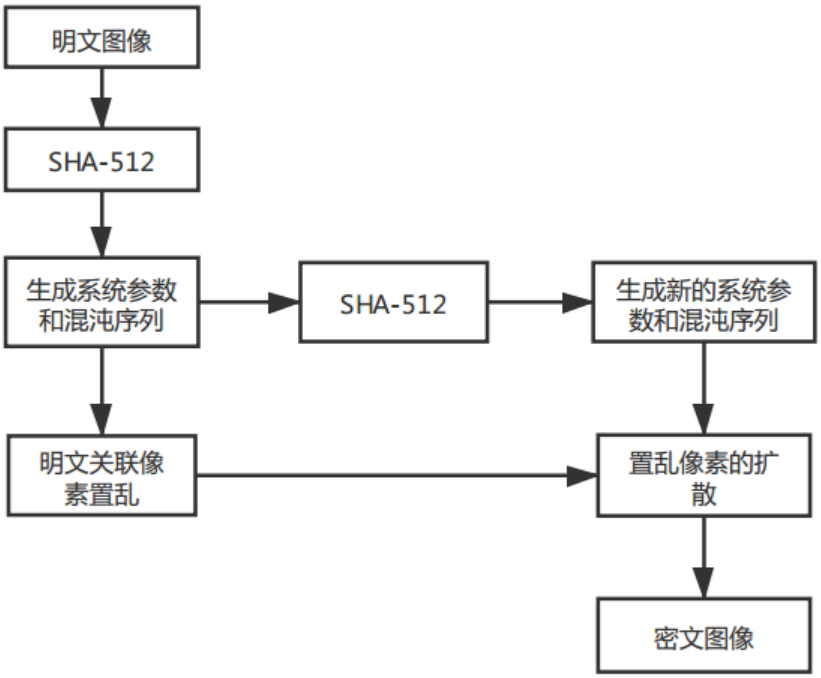


图 4.1 加密算法流程图

4.2.1 像素的置乱

在此次置乱过程中，采用了基于混沌序列的置乱方法来替换原方案的 Arnold 置乱，其具体步骤如下：

步骤 1：将明文图像 $I_{M\times N}$ 作为 SHA-512 函数的输入函数，得到 512 位的二进制哈希值 S_1。

步骤 2：把哈希值 S_1 按照从左到右的原则平均分割成四个二进制数值，每个二进制数值 128 位，分别记为 $X_n=\{X_1,X_2,X_3,X_4\}$。

步骤 3：根据 X_n 计算出混沌序列的初始值，计算公式如下：

$$x_n=\frac{\left(hex2dec\left(X_n\right)\bmod 256\right)}{256},n=1,2,3,4 \tag{4.1}$$

其中 $hex2dec(a)$ 表示将 a 由二进制转化为十进制。

步骤 4：把混沌系统初始值 x_1,x_2,x_3,x_4 代入到 Chen 超混沌系统中进行迭代 $T+M\times N$ 次，得到产生的四个混沌序列，其中 T 的计算公式如下：

$$T=\sum_{n=1}^{4}\left(hex2dec\left(X_n\right)\right)\bmod 256 \tag{4.2}$$

步骤 5：对于得到的步骤四中的四个混沌序列，舍弃每个序列的前 T 个数值以避免暂态效应，得到新的混沌序列，分别记为 $K_n=\{k_1,k_2,k_3,k_4\}$。

步骤 6：对原始明文图像进行置乱，得到置乱后的明文图像，置乱公式如下：

$$\begin{cases} i' = i + \left(abs\left(k_1(i)\right) - \left\lfloor abs\left(k_1(i)\right) \right\rfloor \right) \times 10^{15} \bmod (M - i) \\ j' = j + \left(abs\left(k_1(i)\right) - \left\lfloor abs\left(k_1(i)\right) \right\rfloor \right) \times 10^{15} \bmod (N - i) \end{cases} \tag{4.3}$$

其中(i, j)代表原始明文图像的像素位置，(i', j')代表置乱后的图像的像素位置，$abs(a)$函数代表a的绝对值。

4.2.2 像素的动态扩散

在传统的扩散算法中，部分算法对于像素的扩散并不彻底，还有部分扩散算法的系统参数总是固定的，这样会对系统的安全性造成一定的威胁。因此本方案提出了一种层级密钥的动态扩散方案。在扩散阶段，密钥和系统参数都和置乱阶段的系统参数相关，并且密文之间前后像素相关联，极大的提高了扩散算法的安全性。其具体步骤如下：

步骤 1：对于像素置乱阶段的步骤五中得到的混沌序列k_2，将其按照行列优先的顺序转换成$M \times N$的矩阵，再把矩阵作为 SHA-512 函数的输入，得到 512 位的二进制哈希值S_2。

步骤 2：对于得到的哈希值S_2按照公式 4.1 计算得到新的混沌系统初始值$x'_n = \{x'_1, x'_2, x'_3, x'_4\}$和$T'$，把混沌系统初始值代入到 Chen 超混沌系统中迭代$T' + M \times N$次，舍弃前T'个混沌序列值，得到新的混沌序列，记为$K'_n = \{k'_1, k'_2, k'_3, k'_4\}$。

步骤 3：把置乱后的图像转化为一维的序列，记为$L = \{l(1), l(2), \ldots, l(MN)\}$。

步骤 4：选取混沌序列k'_1来对一维序列L进行加密操作，加密公式如下：

$$E(i) = \left(\left\lfloor \left| k'_1(i) \right| \times 1000 \times (F+1) \right\rfloor - l(i) \right) \bmod (F+1), i = 1, \cdots, M \times N \tag{4.4}$$

其中F表示原始图像的像素最大值，$|a|$表示取a的绝对值，$\lfloor a \rfloor$表示对a向下取整，E表示加密后的一维序列。

步骤 5：把混沌序列k'_2转换成对应的序列R，转换公式如下:

$$R(i) = \left(k'_2(i) \times 10^{15} \right) \bmod 7 + 1, i = 1, 2, \cdots, M \times N \tag{4.5}$$

步骤 6：把一维序列E转换成对应的二进制序列E'，然后进行循环移位操作得到序列C，移位公式如下：

$$C(i) = circshift\left[E'(i), LSB\left(R'(i)\right), R(i) \right], i = 1, \cdots, M \times N \tag{4.6}$$

其中$circshift[u, q, v]$表示对序列u进行v比特的循环移位操作，当$q = 0$时对其

进行向左的循环移位，当$q=1$时对其进行向右的循环移位。*LSB* 函数表示二进制数字的最低有效位，序列R'为序列R的二进制表示。

步骤 7：将序列C转换成最终的密文序列，转换公式如下：

$$\begin{cases} C'(1)=C(1)\oplus\left(\left\lfloor\dfrac{X_1+X_2+X_3+X_4}{4}\right\rfloor \bmod 256\right) \\ C'(i)=C(i)\oplus C(i-1) i=2,\cdots,M\times N \end{cases} \tag{4.7}$$

步骤 8：将一维序列C'转换成二维图像输出，得到最终的加密图像。

4.2.3 图像解密

图像的解密过程为加密过程的逆操作，其大致步骤如下：

步骤 1：根据密钥求出置乱阶段的系统参数和混沌系统的初始值，再根据密钥矩阵求出扩散阶段的系统参数和新的混沌系统初始值。

步骤 2：根据混沌系统初始值迭代求出混沌序列，把密文图像转换成一维序列，对该序列进行逆向解密操作得到序列C，解密公式如下：

$$\begin{cases} C(1)=C'(1)\oplus\left(\left\lfloor\dfrac{X_1+X_2+X_3+X_4}{4}\right\rfloor \bmod 256\right) \\ C(i)=C'(i)\oplus C(i-1) i=2,\cdots,M\times N \end{cases} \tag{4.8}$$

步骤 3：根据求出的混沌序列，对序列C进行逆向比特移位恢复出二进制序列E'，再将二进制序列E'转换成十进制序列E。

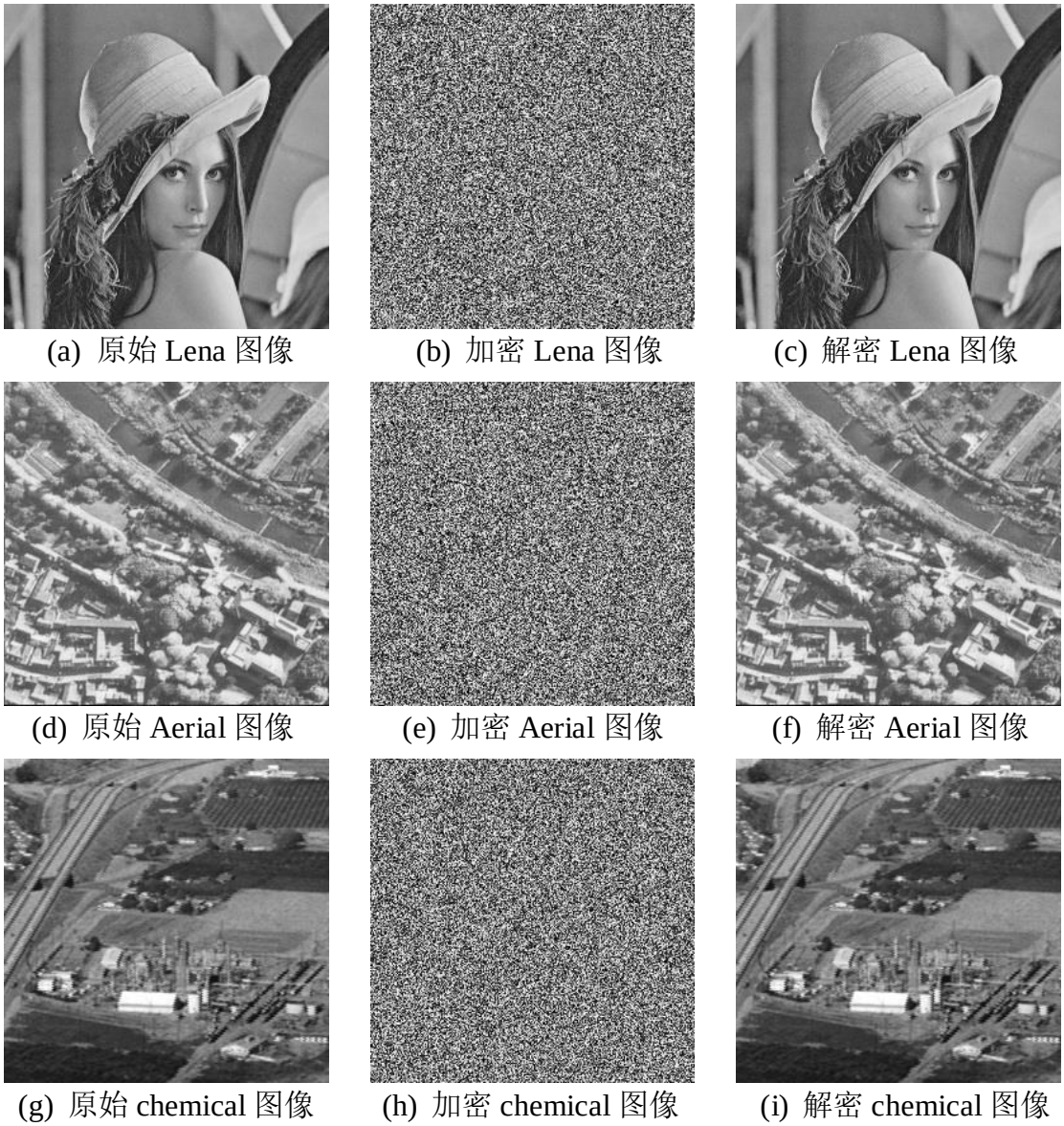
步骤 4：对十进制序列E进行解密操作，解密公式如下：

$$l(i)=\left(\left\lfloor\left|k_1'(i)\right|\times 1000\times(F+1)\right\rfloor-E(i)\right)\bmod(F+1), i=1,\cdots,M\times N \tag{4.9}$$

步骤 5：把序列L转换成图像，再进行置乱，恢复出原始明文图像。

4.3 实验仿真和性能分析

为了测试加密算法的性能，本实验中选取了 8 位 256 色的 Lena 图像、chemical 图像、Aerial 图像，图像大小格式为256×256。其加密和解密结果如图 4.2 所示，从图中可以看出，加密后的图像不能直观的获取有关明文像素有关的信息，并且该加密方案适用于任何格式的图像，应用范围较为广泛。



(a) 原始 Lena 图像　(b) 加密 Lena 图像　(c) 解密 Lena 图像

(d) 原始 Aerial 图像　(e) 加密 Aerial 图像　(f) 解密 Aerial 图像

(g) 原始 chemical 图像　(h) 加密 chemical 图像　(i) 解密 chemical 图像

图 4.2 Lena、Aerial 和 chemical 加解密图像

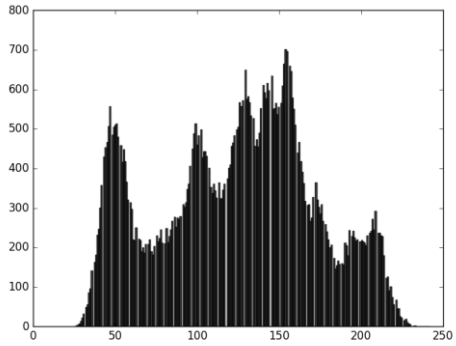
4.3.1 密钥空间分析

为了抵抗来自攻击者的穷举分析，一个良好的图像加密算法应当具有足够大的密钥空间。在本实验方案中，混沌系统初始值和系统参数都是根据明文图像的哈希值计算出来的，因此该算法密钥空间为2^{512}，密钥空间足够大，表明该方案具有良好的抵御穷举攻击的能力。

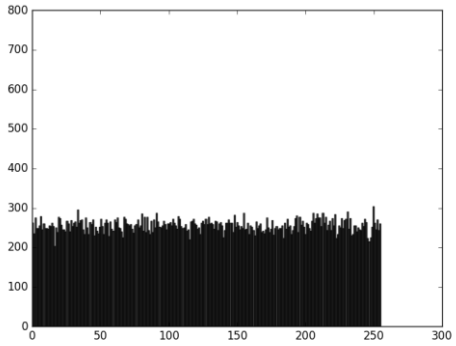
4.3.2 直方图分析

图像的直方图能够清晰的显示出图像本身的统计信息。通过对明文图像和密文图像的直方图作对比，可以判断出该算法能否抵御统计分析攻击。一般而言，对

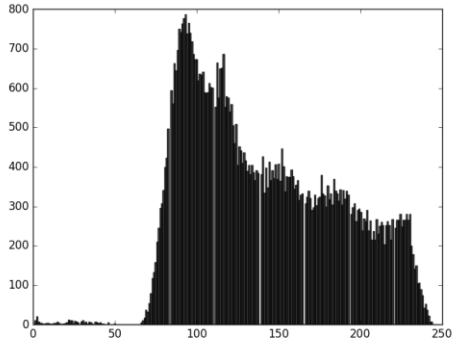
于明文图像的直方图都会存在一定的统计规律，当对明文图像加密后得到密文图像，对密文图像的直方图进行分析，当密文图像的直方图分布愈趋近于平滑，则表明该算法抵御统计分析攻击的能力越强。图 4.3 为原始明文图像和其对应的密文图像的直方图。从图 4.3 中可以看出，加密后的图像直方图分布比较均匀，该算法具有良好的抵御统计分析攻击的能力。



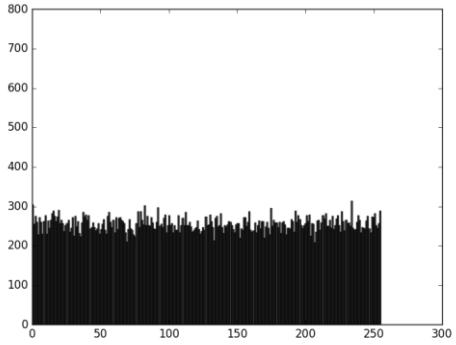
(a) Lena 明文直方图



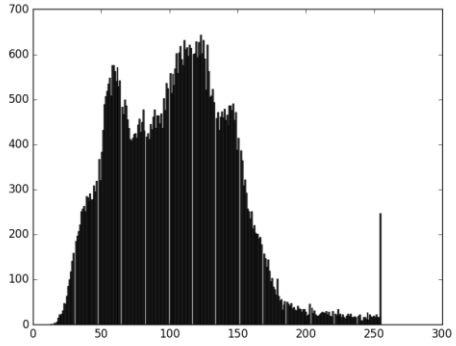
(b) Lena 密文直方图



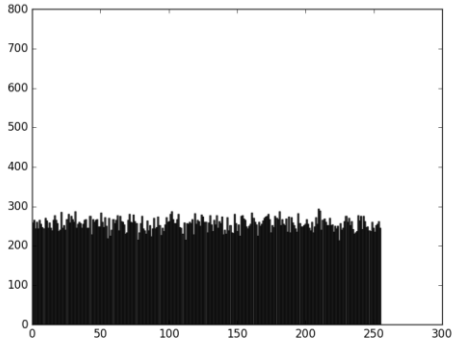
(c) aerial 明文直方图



(d) aerial 密文直方图



(e) chemical 明文直方图

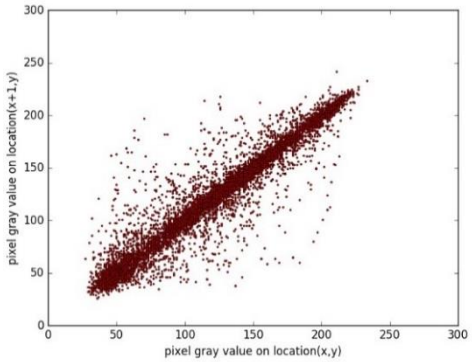


(f) chemical 密文直方图

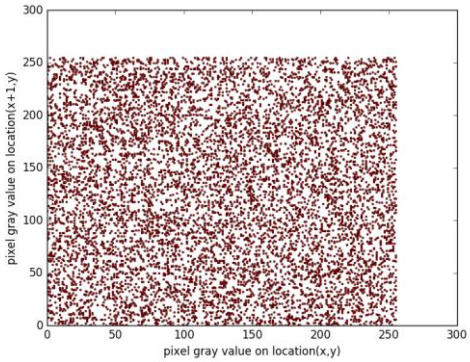
图 4.3 统计直方图

4.3.3 相邻像素相关性分析

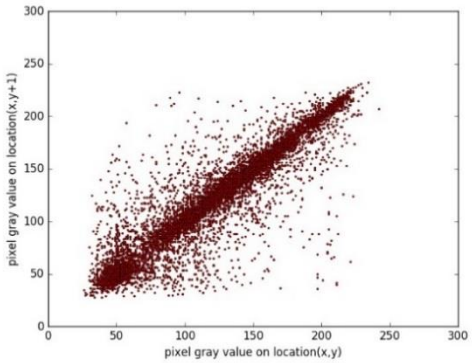
由于图像像素的自身特性，相邻像素间有着很强的相关性。对于一个良好的加密算法而言，加密后的图像的相邻像素的相关性越低越好。本实验中对 Lena 图像的明文和密文图像进行检测分析，随机选择其水平、垂直和对角线三个方向的相邻像素进行分析，图 4.4 展示了 Lena 明文像素和密文像素的分布情况，表 4.1 展示了明文像素和加密图像的像素相关性，并与别的方案进行比较。



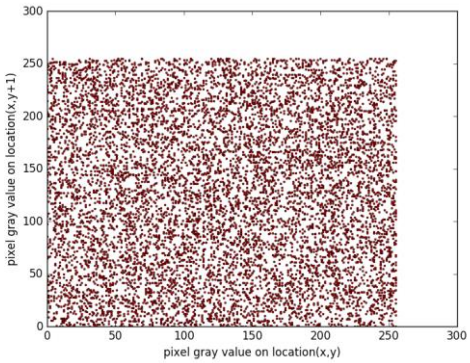
(a)明文水平方向



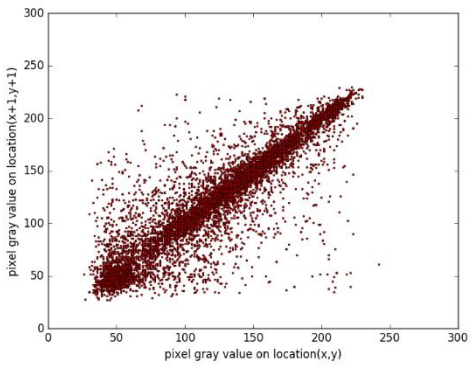
(b) 密文水平方向



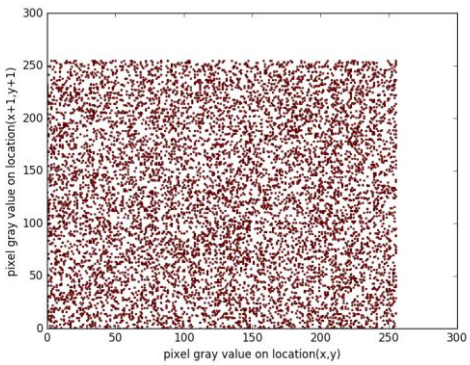
(c) 明文垂直方向



(d) 密文垂直方向



(e) 明文对角方向



(f) 密文对角方向

图 4.4 相邻像素点的相关性分析

表 4.1 相邻像素相关系数

方向	明文图像	本文算法	[47]	[48]
水平	0.956	-0.0054	0.0272	0.0214
垂直	0.916	0.0013	-0.0114	0.0465
对角	0.901	0.0201	-0.0484	-0.009

上述结果表明，明文图像像素间的相关性较强，加密后的密文图像像素间的相关系数较低，与其它方案相比，本加密算法降低像素的相关性效果更好。

4.3.4 信息熵分析

信息熵是用来衡量信息随机性的重要指标之一，在本方案中，对 Lena 明文图像进行加密，并计算其信息熵，表 4.2 展示了计算的密文信息熵大小，并与其它的方案进行比较，结果表明本加密算法使得加密后的密文图像像素均匀分布。

表 4.2 信息熵比较

方案	本算法	[50]	[49]	[47]
Lena	7.9975	7.997067	7.9967	7.9964

4.3.5 差分攻击分析

一个良好的图像加密算法应具有较强的抵御差分攻击的能力。一般而言，评价图像抵御差分攻击能力有两个重要指标，像素改变率(NPCR)和平均一直改变强度(UACI)。在本方案中，根据公式 2.17 和 2.18 计算密文的 UACI 和 NPCR 值。表 4.3 展示了本方案加密后的 Lena 图像的 UACI 和 NPCR 值，并与其它的方案进行了比较。最终的实验结果表明，密文 Lena 图像的 UACI 和 NPCR 值都比较接近理想值 33.4635%和 99.6094%，表明该算法能有效的抵御差分攻击。

表 4.3 测试图像的 UACI 和 NPCR 值

方案	UACI 值	NPCR 值
本算法	33.45%	99.57%
[49]	28.27%	99.54%
[48]	33.44%	99.58%

4.3.6 密钥敏感性测试

密钥敏感性测试是指当密钥发生微小的变化时，对明文图像进行加密或解密，

得到的两个图像的差别情况。在本次仿真分析中，以测试题 Lena 为例，图 4.5 展示了当加密密钥发生微小的改变时，Lena 密文图像和用原始密钥加密的密文 Lena 图像的不同点。

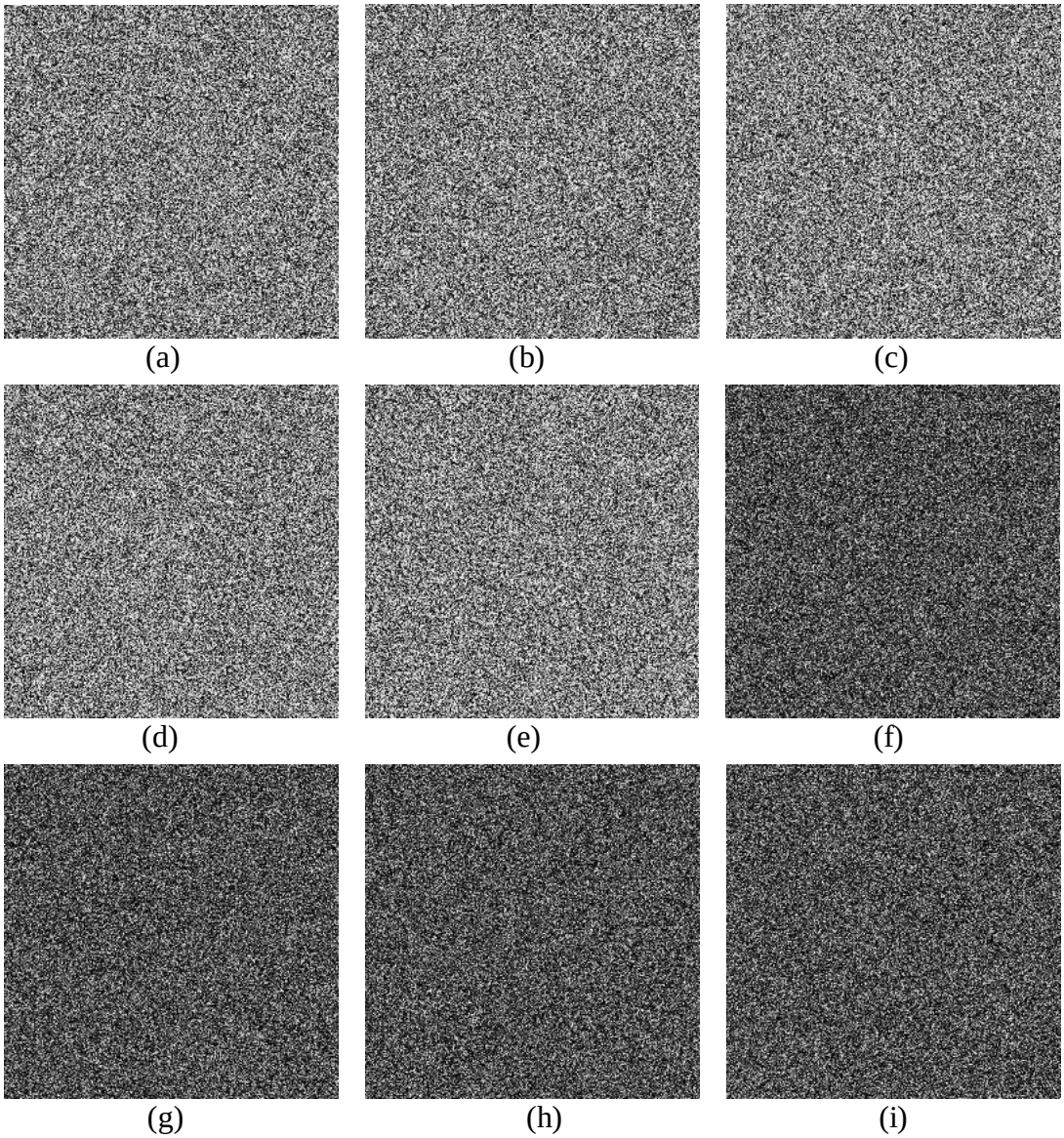


图 4.5 密钥敏感性测试

在上述图片中，图片 a 表示用原始密钥加密 Lena 图像后得到的加密图像，图片 b、c、d、e 代表初始混沌密钥发生微小改变时，即 x_1+10^{-6}、x_2+10^{-6}、x_3+10^{-6}、x_4+10^{-6} 时加密得到的 Lena 密文图像。图片 f、g、h、i 表示图像 a 和 b、c、d、e 的差异。从中可以看出，当密钥发生微小的改变时，得到的密文图像和正确的密文图像差异较大，表明该算法具有较强的密钥敏感性。

4.4 本章总结

本章在第三章的基础上，本章设计了一种基于 Chen 超混沌系统的明文关联图像加密算法。首先利用明文图像作为 SHA-512 函数的输入，产生了 512 位的哈希值，然后基于此哈希值计算出混沌系统的初始值和系统参数。在置乱阶段，采用一种基于混沌序列的置乱方法来对原始图像进行置乱，然后在扩散阶段重新生成新的混沌系统初始值和系统参数，最后通过对密文的比特移位操作和密文间的异或操作来加强密文对明文的敏感性，最后输出加密后的图像。实验结果表明，该算法密钥空间大，对密钥敏感性强，并且对统计分析攻击、差分攻击和选择明文攻击都有较强的抵御能力，相比于第三章的算法而言，本章节中提出的算法性能都有明显的改善。

第五章 结论和展望

5.1 结论

在互联网信息技术蓬勃发展的今天，图像已成为一种重要的信息载体在人类社会中广泛传播，例如医生通过网络传递病人的带有个人疾病信息的隐私照片，警察通过网络传递犯罪分子的个人肖像照片等。如果通过信息安全技术来实现图像在互联网中的安全传播已经成为世界学者的研究热点之一。香农曾指出，一个良好的加密系统应该包含两部分：置乱和扩散。对于图像加密而言，置乱是改变像素的空间分布规律，扩散是指改变像素之间的统计特性。在 1989 年英国数学家 Robert A.J.Matthews 首次把混沌系统应用到信息加密领域当中，混沌系统的这一成功应用为后续的学者提供了新的研究方向。经过研究发现，混沌系统具有随机性强、对初值敏感性等特点，因此适用于图像加密当中。经过对混沌系统进行更进一步的研究，学者发现混沌系统分为低维混沌系统和高维混沌系统。其中低维混沌系统具有效率高、迭代速度快等优点，但是相对的由于其维度低，系统较为简单，因此其安全性不高，易于遭到攻击者的破解。而高维的混沌系统虽然安全性较高，同时具有更为复杂的运动行为，对初始值更强的敏感性，但是其迭代效率不高。本文主要研究 Chen 超混沌系统在图像加密中的应用，总结了有关国内外的加密成果，并提出了两种基于 Chen 超混沌系统的加密算法，通过相关实验和仿真分析比较算法的性能。主要研究工作如下：

首先，本文陈述了图像加密的相关背景和研究意义，指出了混沌系统的特点以及国内外的学者的研究现状，列举了部分基于混沌系统的图像加密的研究成果，指出与低维混沌系统相比，超混沌系统具有更为复杂的运动学行为，更高的安全性，因此更适用于图像加密领域当中。

然后，本文介绍了有关混沌理论的基本特征，图像加密和文本加密的异同点，对本文中使用的 Chen 超混沌系统进行了仿真分析，以及列举了图像加密的算法性能的评价标准。

其次，本文提出了基于 Chen 超混沌系统的图像加密算法，该算法利用 Arnold 置乱来对明文图像进行置乱操作，然后利用产生的混沌序列来对置乱后的图像进行扩散，最终的实验结果表明，虽然图像的加密效果较好，但是分析发现系统内的各种参数都是固定的，密文对明文的敏感性不强，无法抵御选择明文攻击。而且在

图像置乱阶段采用的 Arnold 置乱，只适用于正方形格式的图片，有一定的局限性。同时加密后的图像的像素相关性偏高，易遭到攻击者的破解，因此需要对加密算法作出一定的改进。

最后，基于前面提出的图像加密算法的缺点，通过进一步对有关混沌系统图像加密技术的研究，提出了一种基于 Chen 超混沌系统的明文关联图像加密方案。在该加密算法中，首先采用了一种基于混沌序列的置乱方法，该置乱方法适用于任意格式的图片。然后利用 SHA-512 函数对原始明文图像进行哈希，得到 512 位的二进制哈希值，系统内的各种参数和混沌系统初始值都是根据此哈希值计算得出。在图像的扩散阶段，通过像素之间的异或操作来加强明文和密文像素的敏感性。最终实验结果表明，该算法不仅能抵御选择明文攻击和差分攻击，同时具有较大的密钥空间，具有较好的安全性。

5.2 展望

虽然本文提出了一种基于 Chen 超混沌系统的明文关联图像加密方案，相比于原先的加密算法性能有了一定的提升，但是由于自身科研水平有限，研究工作还需更进一步的完善：

（1）提高系统加密效率。与低维混沌系统相比，虽然超混沌系统具有更为复杂的运动学行为，更高的安全性，但是与此同时，它的迭代效率降低了。应该进一步研究克服安全性和效率之间的矛盾，提高算法性能。

（2）本文提出的算法都是基于空间域进行的，基于变换域、机器学习和压缩感知等领域都是当前研究的热点领域，通过和其它的领域相结合，以求达到对加密算法的不断创新与改进。

（3）在实际应用中存在的噪音问题。当图像在网络中进行传输时，或多或少都会受到来自外界或内在因素的干扰，因此会对密文造成一定的影响。所以要考虑加强算法的抗噪音能力，使其对噪音干扰具有一定的抵抗力。

参考文献

[1] Xiao S, Guo Y, Huang K, et al. Cooperative group secret key generation based on secure network coding[J]. IEEE Communications Letters, 2018, 22(7): 1466-1469.

[2] Stallings W. 密码编码学与网络安全: 原理与实践, 第二版[M]. 电子工业出版社, 2001.

[3] Chai X, Chen Y, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations[J]. Optics and Lasers in engineering, 2017, 88: 197-213.

[4] 贾铁军, 蒋建军. 网络安全技术及应用实践教程[M]. BEIJING BOOK CO. INC., 2018.

[5] Li C. Cracking a hierarchical chaotic image encryption algorithm based on permutation[J]. Signal Processing, 2016, 118: 203-210.

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

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

[8] Shannon C E. A mathematical theory of communication[J]. Bell system technical journal, 1948, 27(3): 379-423.

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

[10] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and chaos, 1998, 8(06): 1259-1284.

[11] Zhang Y, Tang Y. A plaintext-related image encryption algorithm based on chaos[J]. Multimedia Tools and Applications, 2018, 77(6): 6647-6669.

[12] Wu J, Tu L. An image encryption algorithm based on Josephus traversing and position disordering[C]//Proceedings of the 2012 International Conference on Cybernetics and Informatics. Springer, New York, NY, 2014: 1941-1946.

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

[14] Wang X, Liu L, Zhang Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique[J]. Optics and Lasers in Engineering, 2015, 66: 10-18.

[15] Akhshani A, Akhavan A, Lim S C, et al. An image encryption scheme based on quantum logistic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(12): 4653-4661.

[16] Ye G, Huang X. An efficient symmetric image encryption algorithm based on an intertwining logistic map[J]. Neurocomputing, 2017, 251: 45-53.

[17] Yang B, Liao X. A new color image encryption scheme based on logistic map over the finite field Z N[J]. Multimedia Tools and Applications, 2018, 77(16): 21803-21821.

[18] 程欢欢,戴曙光,杨莹.基于三维 Arnold 的 Logistic 混沌系统图像加密[J].电子测量技术,2019,42(22):135-139.

[19] Han C. An image encryption algorithm based on modified logistic chaotic map[J]. Optik, 2019,

181: 779-785.

[20] Patel S, Muthu R K. Image Encryption Decryption Using Chaotic Logistic Mapping and DNA Encoding[J]. arXiv preprint arXiv:2003.06616, 2020.

[21] Li Z, Peng C, Li L, et al. A novel plaintext-related image encryption scheme using hyper-chaotic system[J]. Nonlinear Dynamics, 2018, 94(2): 1319-1333.

[22] Luo Y, Zhou R, Liu J, et al. A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map[J]. Nonlinear Dynamics, 2018, 93(3): 1165-1181.

[23] Zhu H, Zhao Y, Song Y. 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption[J]. IEEE Access, 2019, 7: 14081-14098.

[24] Stalin S, Maheshwary P, Shukla P K, et al. Fast and Secure Medical Image Encryption Based on Non Linear 4D Logistic Map and DNA Sequences (NL4DLM_DNA)[J]. Journal of medical systems, 2019, 43(8): 267.

[25] Xu J, Li P, Yang F, et al. High Intensity Image Encryption Scheme Based on Quantum Logistic Chaotic Map and Complex Hyperchaotic System[J]. IEEE Access, 2019, 7: 167904-167918.

[26] Zhang G, Ding W, Li L. Image Encryption Algorithm Based on Tent Delay-Sine Cascade with Logistic Map[J]. Symmetry, 2020, 12(3): 355.

[27] Sun S, Guo Y, Wu R. A novel image encryption scheme based on 7D hyperchaotic system and row-column simultaneous swapping[J]. IEEE Access, 2019, 7: 28539-28547.

[28] Chen G, Mao Y, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals, 2004, 21(3): 749-761.

[29] Zhang X, Wang X. Digital image encryption algorithm based on elliptic curve public cryptosystem[J]. IEEE Access, 2018, 6: 70025-70034.

[30] Zhen P, Zhao G, Min L, et al. Chaos-based image encryption scheme combining DNA coding and entropy[J]. Multimedia Tools and Applications, 2016, 75(11): 6303-6319.

[31] Zhang H, Wang X, Wang X, et al. Novel multiple images encryption algorithm using CML system and DNA encoding[J]. IET Image Processing, 2019, 14(3): 518-529.

[32] Wan Y, Gu S, Du B. A New Image Encryption Algorithm Based on Composite Chaos and Hyperchaos Combined with DNA Coding[J]. Entropy, 2020, 22(2): 171.

[33] Ponuma R, Amutha R. Encryption of image data using compressive sensing and chaotic system[J]. Multimedia Tools and Applications, 2019, 78(9): 11857-11881.

[34] Yao S, Chen L, Zhong Y. An encryption system for color image based on compressive sensing[J]. Optics & Laser Technology, 2019, 120: 105703.

[35] ur Rehman A, Liao X, Ashraf R, et al. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2[J]. Optik, 2018, 159: 348-367.

[36] 刘西林, 严广乐. 基于明文相关的混沌映射与 SHA-256 算法数字图像的加密与监测[J]. 计算机应用研究, 2019, 36(11): 3401-3403, 3414.

[37] Kar M, Kumar A, Nandi D, et al. Image encryption using DNA coding and hyperchaotic system[J]. IETE Technical Review, 2018: 1-12.

[38] 田强宝, 谢冬. 基于压缩感知和随机像素置换的多图像联合加密方案[J]. 杭州师范大学学报(自然科学版), 2020, 19(02): 208-214.

[39] Fu C, Zhang G Y, Zhu M, et al. A Fast Chaos-Based Colour Image Encryption Algorithm Using a Hash Function[J]. Informatica, 2018, 29(4): 651-673.

[40] Sun S. A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling[J]. IEEE Photonics Journal, 2018, 10(2): 1-14.

[41] Tien-Yien L, Yorke J A. Period three implies chaos[J]. Am Math Monthly, 1975, 82: 985-992.

[42] Devaney R L. An introduction to chaotic dynamical systems[J]. 1989.

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

[44] Hénon M. A two-dimensional mapping with a strange attractor[M]//The Theory of Chaotic Attractors. Springer, New York, NY, 1976: 94-102.

[45] Wang X Y, Wang M J. Hyperchaotic Lorenz system[J]. 2007.

[46] 王可, 张红伟, 李晓辉. 基于 DNA 编码运算和混沌系统的图像分块加密算法[J]. 电视技术, 2017, 41(03): 6-10.

[47] Wang W, Si M, Pang Y, et al. An encryption algorithm based on combined chaos in body area networks[J]. Computers & Electrical Engineering, 2018, 65: 282-291.

[48] Zhen P, Zhao G, Min L, et al. Chaos-based image encryption scheme combining DNA coding and entropy[J]. Multimedia Tools and Applications, 2016, 75(11): 6303-6319.

[49] Huang C K, Liao C W, Hsu S L, et al. Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system[J]. Telecommunication Systems, 2013, 52(2): 563-571.

[50] Ye G, Pan C, Huang X, et al. An efficient pixel-level chaotic image encryption algorithm[J]. Nonlinear Dynamics, 2018, 94(1): 745-756.

致谢

转眼之间，研究生三年已快结束了，可以说自己的读书生涯已经差不多彻底结束了，以后自己将步入社会。这一切仿佛来得很快，也很突然，想到三年前自己迈入硕士的大门，如今写下这篇毕业论文，也算是为自己的三年的学习划上一个句号。

在这三年的时光里，我收获颇丰。首先要感谢自己的导师张明武老师，他引导我迈入了密码学这个新的学科的大门。在学术上，他经常联系校外专家来实验室进行讲座，极大的开阔了我们的视野，丰富了我们的知识面；在生活上，他对我们实验室的每个人都照顾有加，关系着我们的成长。他自身的对待科研的严谨的态度，一丝不苟的做事风格深深的影响了我，激励着我不断成长。其次要感谢实验室的李兵兵老师，每一次的研讨会，她都多次和我反复讨论，对于我不明白的知识点，和我细致的研讨，直到我完全明白，可以说是良师益友。

最后，要感谢整个实验室里面的沈华老师、赵岚老师、张媛媛老师、刘白老师、谌刚老师、陈永辉老师等，还有上一届的师兄师姐们，以及本届的实验室的同门，感谢他们对我的曾经的帮助和支持。