摘 要

混沌映射具有良好的不可预测性、遍历性和对参数的敏感性，在图像安全领域得到了广泛的应用。本文引入了一个新的 Sine-Henon 映射(ICSM)，它是由 Sine 映射和 Henon 映射级联而成的。和目前大多数的混沌映射相比，它拥有好的混沌特性并且更容易实现。为了研究它在图像安全领域的加密性能，一种混沌奇异变换(CMT)方法被提出，该方法可以有效地置乱图像像素。结合 ICSM 和 CMT，本文设计了一种新的图像加密算法。模拟结果和安全性分析都表明，该算法在面对不同的图片时，都具备良好的加密特性和较稳定的抗干扰性，并能防御各种常见的攻击，另外，为了更好地将研究的算法投入到实际应用中，设计了一款图像加密系统的 GUI。最后，对所有的工作进行了总结与展望。

关键词：图像加密；混沌映射；CMT 变换；置乱；扩散

ABSTRACT

Chaotic maps have been widely used in the field of image security due to their good unpredictability, ergodicity and sensitivity to parameters. In this paper, we introduce a new Sine-Henon map (ICSM), which is a cascade of Sine map and Henon map. Compared with most of the current chaotic maps, it has good chaotic properties and is easier to implement. In order to study its encryption performance in the field of image security, a Chaotic Magic Transform (CMT) method is proposed, which can effectively disrupt image pixels. Combining ICSM and CMT, a new image encryption algorithm is designed in this paper. After simulating and analyzing their security, results show that the proposed algorithm has good encryption characteristics and more stable anti-interference when facing different images, and can defend against various common attacks. In addition, a GUI of the image encryption system is designed in order to better put the studied algorithm into practical applications. Ultimately, all the work is summarized and prospected.

Keywords: Image encryption, Chaotic maps, CMT transform, Permutation, Diffusion

目录

第 1 章 绪论

1.1 课题研究背景和意义

近年来，信息安全已经成为了一个热门的研究领域，我们日常生活中的许多行为都处于数字化的环境中。保护数据的主要参考来源是密码学，在这个多学科领域中，提出一个新的保密算法/协议是一个挑战，一旦加密方式稍有不慎，很可能被试图窃取信息的人有了可乘之机，如2017年加拿大贝尔遇黑客袭击，导致用户数据遭泄露，大概有190万个使用中的电子邮件地址，接近1700名客户的名字和使用的电话号码被非法访问，事情被曝光后，各国也加强了对信息安全的重视程度[1]。目前，随着网络通信技术的发展，尤其是当前逐渐普及的5G技术，图像视频信息已经占据了网络信息的70%[2]。因此，数字图像(Digital Image)，作为一种特殊的信息表达载体形式，因而保护图像中的隐私信息就显得十分的重要[3]。

主要有两种用于保护数字图像隐私安全的传统方法：图像数字水印和图像加密。前者主要是指在明文图像(Plaintext Image)中嵌入数字水印，以保护相关明文图像的版权。后者主要是通过具体的可逆数学变换对图像的像素位置和像素值进行操作，使得变换前后的数字图像尽量不相关，从而阻止未授权的第三方获取到明文图像的具体内容信息[4]。

当前用来保护图像隐私安全的方法大多都是采用图像加密，图像加密有很多种方式，我们可以通过互联网、彩信等方式发送加密图像。图像加密用于将普通图像转换成密码图像，用来保护信息免受非法访问[5-7]，一般会在像素值改变的阶段，进行数据加密以确保安全性，每个像素用数值表示，像素单位大小等于图像大小除以矩阵大小，矩阵尺寸是每副图像的长度和宽度的像素数，每个像素位置上的像素值是图像在该处的灰度值。通过利用一些加密算法和密钥，可以将原始图像改变为不被任何未授权的人访问的普通图像。传统的加密算法，如DES(Data Encryption Standard)、AES(Advance Encryption Standard)[8]，但这些算法加密结果信息量大、相邻像素间的关联性强，不适合用于图像加密。特别地，因为混沌系统有如下独特性质：因初值和参数的变化引起轨迹的大幅变化，还有它的不可预测性，混沌系统的这些特性自然与密码学中的置乱和扩散特性相关，混沌系统对初始状态的高度敏感性，与密码学系统对密钥的极端敏感性相似，此外，不可预测性也符合密码系统的扩散特性，所以混沌系统现已在图像信息安全领域中被广泛地应用，并已成为近年来图像加密领域的热点问题之一 [9-10]。

1.2 课题研究现状

利用混沌映射具有的这些特性，研究者用它们来生成具有不同参数或初始值设置的不同随机序列，也是因为这一优势，混沌映射引起了更多研究者的关注，并在不同的应用领域得到了广泛的应用。

在安全应用中，混沌映射现出了优异的性能，例如，Zhu等人[11]提出了使用Arnold Cat映射对称图像加密方案。Zhang等人[12]提出的基于混合线性-非线性耦合映射对称图像加密算法，Zhou等人[13]提出了一个新的1-D混沌系统的图像加密算法。绝大多数情况下，分为两种类型的混沌映射：一维(1-D)混沌映射和高维(H-D)混沌映射。1-D混沌映射通常参数少，实现起来较为容易，例如Logistic映射、Gauss映射、Sine映射和Tent映射[14]。对比其它映射来说，它们的构造方式是极为简单的。21世纪以来，不少学者对混沌轨迹预测技术进行了大量研究，发现即便在提取信息较少的情况下，也可以对这些简单的混沌映射轨迹进行估计[15]，并且能较好的估计其参数的初始值。正是因为这些缺陷，它们在许多安全领域的应用被限制了。例如，当1-D混沌映射用于图像加密时，有几种加密算法是保密性能较差的[16]。被证明安全性不强的还有文献[17]中提出的一种基于Logistic映射的图像加密算法。而相对来说，H-D混沌映射的加密性能更好，H-D混沌映射的典型例子有Henon映射，Lorenz系统和Chee-Lee系统[18]。与1-D混沌映射相比，H-D混沌映射通常具有更优越的混沌性能，但它们很难在实际中实现，并且计算的速度对比低维映射的计算速度也较慢。因此，开发一种具有良好混沌性能且实现成本较低的混沌图像加密算法具有重要意义[19]。

1.3 论文主要研究内容及结构安排

本文创新地提出了一种级联混沌系统，称为 Sine-Henon 映射(ICSM)。它是由一个一维混沌映射和一个二维映射组合而成的。性能分析表明，对比现有的混沌映射，在同等计算成本条件约束下，ICSM 具有混沌范围更宽广、遍历性以及更好的混沌性能等优势。为了展示 ICSM 在安全应用中的性能，本文提出了一种用于图像加密的混沌奇异变换(CMT)。CMT 利用 ICSM 生成的混沌序列，能够同时在行和列两个方向上对图像像素进行快速置乱。结合 ICSM 和 CMT，本文创新地设计了算法结构，提出了一种新的基于 CMT 的图像加密算法(CMT-ICSM)。另外，为了验证算法在实际应用中的各种性能，本文对提出的算法进行了安全性分析，确保其具有良好的安全性与抗干扰性。最后，为使算法能较为方便地供日常使用，本文设计了一款 GUI 供用户使用，不仅能作为加密系统加密信息，还能供科研人员测试与开发，提升进行科学研究的效率。全文共分五个章

节，下面对每一章的主要内容进行阐述：

第 1 章：介绍近年混沌图像算法加密的研究趋势与最新情况，举了近年来很多研究图像算法加密的例子，对比了传统方法与现代方法的优点与缺点，同时也强调了图像加密对于我们日常生活、军事领域安全等方面的重要性。

第 2 章：从混沌的发展、混沌系统的一系列特点和经典的混沌映射出发，介绍了混沌图像算法加密的基本术语与概念，同时也列举了一些常见的攻击图像的方法，这对后续展开针对性的保护信息的研究指明了方向，提供了理论基础。

第 3 章：提出了一种新的混沌系统 CMT-ICSM，同时对该算法的各指标性能进行了安全性分析，使用该算法对不同的图像进行加密，加密结果均表明该算法的性能较好，适用于图像安全领域。

第 4 章：设计了一款图像算法加密系统 GUI，不仅可用于日常传输信息方面，还可为研究人员提供便捷，以促进混沌图像加密领域的发展。

第 5 章：总结了本文所做的工作，并且指出了研究中所存在的不足，以及后续需改进的地方，同时也对该领域的发展提供了一些自己的想法。

第 2 章 混沌图像加密基本理论

2.1 混沌的基本理论

2.1.1 混沌的发展过程

混沌理论是一个跨学科的科学理论和数学分支，主要研究具有完全随机的无序和不规则状态的动力系统中的潜在模式和对初始条件高度敏感的确定性规律。

早期的科学家们也进行了关于混沌的相关研究：例如伯克霍夫的三体问题，科尔莫戈罗夫的湍流和天文问题，以及卡特赖特和利特尔伍德的无线电工程。虽然没有观察到混沌的行星运动，但实验者在流体运动中遇到了湍流，在无线电线路中遇到非周期性的振荡，而没有理论来解释他们所看到的东西[20]。

混沌理论被正式确定下来的时间是本世纪中叶，一些科学家在研究时发现了 Logistic 映射现象，但在当时并无理论能解释该现象，故这被归结为测量不精确和简单的“噪声”。该理论的创始人是美国气象学家 Lorenz，他使用一台数字计算机来对天气进行模拟，但结果发现预测的数据与计算得出完全不同。而 Lorenz 发现，初始条件的细小变化是产生结果巨大变化的原因[21]。1977 年，第一次关于混沌的研讨会由纽约科学院组织，Ruelle、May、Yorke、Shaw 和气象学家 Lorenz 参与了会议[22]。次年，Feigenbaum 发现了混沌的普遍性，允许混沌理论应用于许多不同现象，这标志着混沌理论的诞生。20 世纪末，计算能力更强的计算机的出现扩大了混沌理论的适用范围。也正是因为混沌具有的这些特性，到现在为止，基于混沌系统的信息加密方案拥有十分广阔的发展前景和研究价值。

2.1.2 混沌的定义和特性

在混沌理论中，混沌被更精确地定义了。即便现在混沌的数学定义还没有被普遍承认，但最初由 Devaney 提出的一个普遍使用的定义[23]是，一个混沌系统必备的条件是：(1) 对初始条件敏感 (2) 是拓扑上的传递性 (3)有密集的周期性轨道。而混沌主要有以下这些特性：

(1) 初值敏感性

对初始值和参数敏感。混沌系统初始值和参数值的微小变化可以触发系统未来状态的巨大变化。这种特性非常适合满足密码学的密钥要求，类似于众所周知的“蝴蝶效应”。

(2) 非周期性

混沌运动的状态是不具有周期性的，不同于其他动力学系统的确定性，混沌系统对于几乎所有的初始条件，变量的演化是混沌的，具有非周期性的行为[24]。

(3) 有界性

混沌具有有界性，一个确切的区域里始终存在它的轨迹，称为混沌吸引域。

(4) 遍历性

在混沌吸引域内，混沌运动是会经过各个状态的，换种说法，混沌运动历经混沌吸引域内每一个状态。

(5) 分维性

分维性和一般的运动理论存在不同，混沌系统的运动轨线中，会在一个有限范围内进行无限的折叠，之后又会出现多个单叶、多层次的结构，这也就体现了自相似结构 [25]。

(6) 普适性

在不同的混沌系统在混沌状态时会出现相似的特征，该性质可以在几个特殊的计算指标上体现，如 Feigenbaum 常数等[26]。

(7) 奇怪吸引子特性

一些动力系统，如 Logistic 映射，每个状态都是混沌的，当吸引子上发生混沌时，这个混沌区域的轨迹会有大量的初始条件收敛于此[27]。

2.1.3 混沌系统的判定方法

判断一个系统是否混沌，不能仅从其数学描述得出结论，一般采用如下方法。

(1) Lyapunov 指数法

一个系统若是混沌的，则它其中一个 Lyapunov 值必是正数，如果存在两个以上的 Lyapunov 值，则系统是超混沌的。Lyapunov 指数的数值计算方法有 Wolf 方法，Jacobian 方法等[28]。

(2) Poincare 截面法

把 Poincare 截面定义为在相空间一个截面上某一对共轭变量构成的截面。系统是混沌的现象是 Poincare 截面存在一些成片的具有分形结构的密集点[29]。

(3) 时域及相轨迹的直接观察方法

通过在时域分析里观察各个状态变量的波形，会发现混沌的分岔(bifurcation)和阵发性混沌。

(4) 分维数

我们可以用很少的自由度来描述存在于混沌运动中某种难以观察的规则。混沌自由度会在分维数中表达，并且有很多种分维数的具体形式。

(5) Kolmogorov 熵

可以在相空间中计算关联维数和 Kolmogorov 熵，通常采用最小二乘法等方法。

2.1.4 几种典型的混沌映射

为了理解后续章节提出的混沌映射，这里简单介绍几种混沌映射。

(1) Logistic 映射

在密码学和其他领域使用的最流行的混沌映射之一是 Logistic 映射[30]。这是因为它的计算成本很低，而且只要对其参数进行适当的初始化就能产生混沌。该映射在数学上可以描述为：

$$x_{n+1}=\mu\times x_n\times(1-x_n) \tag{2.1}$$

其中$x\in[0,1],\mu\in[0,4]$。然而，Logistic 映射的混沌参数范围有限，而且会出现分岔状态，像虫口一样，所以 Logistic 映射也称为虫口映射，如后面图 2.1 所示。

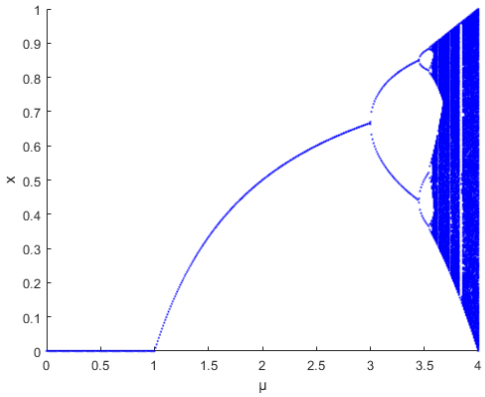


图 2.1 Logistic 映射分岔图

由上图可以看出，Logistic 映射的状态与参数值十分相关，只在特定区间出现混沌。当$3.56994567\cdots<\mu\leqslant 4$时，若混沌映射的初值$x_0\in[0,1]$，并进行若干次计算后，得到一个非周期的数值序列，该序列所有值皆在混沌吸引域内，此时的 Logistic 映射为混沌的。

(2) Sine 映射

这个映射是一个一维混沌映射，该映射在数学上可以描述为：

$$x_{n+1}=a\times\sin(\pi x_n) \tag{2.2}$$

其中$a\in[0,1]$，当$a\in[0.87,1]$时，该映射是混沌的，其混沌分岔图如下图。

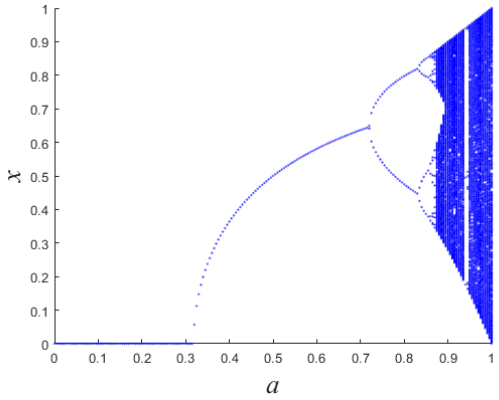


图 2.2 Sine 映射分岔图

(3) Henon 映射

Henon 映射是一种常见的二维映射，被如下数学式定义：

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{2.3}$$

其中a和b是控制参数，x和y是混沌状态。当$a=1.4$和$b=0.3$时，Henon 映射具有混沌行为[31]。图 2.3 显示了 Henon 映射的分岔图，但是可以从图中看出其具有一定的周期性，只有参数值在有限范围内才会产生混沌。此外，Henon 映射的混沌复杂性很低，这个缺陷对于图像加密领域来说是不可忽视的。

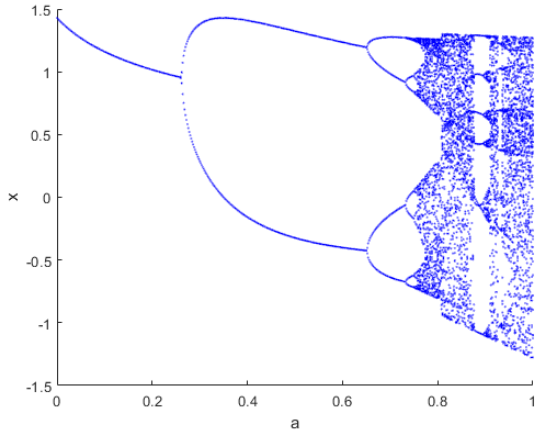


图 2.3 Henon 映射分岔图

2.2 混沌图像加密

2.2.1 密码学的基本概念

通信双方按约定的法则进行信息特殊变形的保密方法，称为密码。加密变换是变明文为密文，而解密变换变密文为明文[32]。如图 2.4 所示，一个密码系统主

要由以下部分组成。

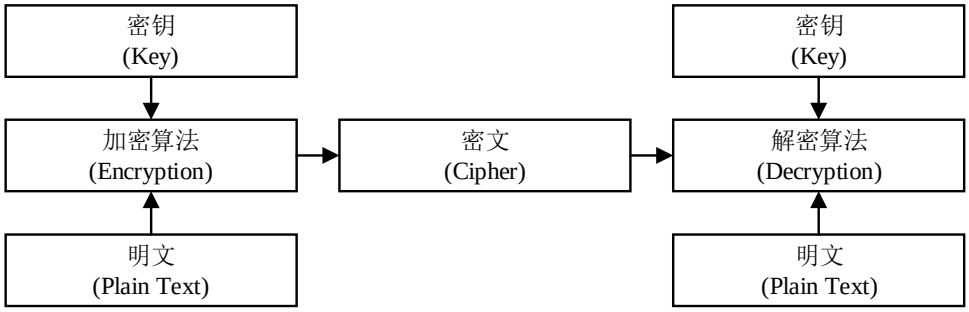


图 2.4 现代密码系统

其中，明文为等待加密的图像信息。密文是经过密钥和加密算法处理后得到的图像信息，无法被外界获取。密钥是在整个流程中所用到的特定参数。加密算法是将明文图像信息处理为加密后图像的方法。解密算法是将密文图像信息处理为解密后图像的方法。

2.2.2 密码分析与攻击的种类

解密者在不知道加密系统的密钥前提下，对加密系统进行分析，通过信息特征破解获得明文信息，称为密码分析，分析类型分为以下几种。

表 2.1 密码分析的类型

分析类型	分析者需掌握的信息
唯密文分析	加密算法 获取的部分密文
已知明文分析	加密算法 获取的部分密文 一个或多个明文密文对
选择明文分析	加密算法 获取的部分密文 选择的明文信息及对应的密文信息
选择密文分析	加密算法 获取的部分密文 选择的密文信息及对应的被解密的明文信息

最常见的密码攻击有如下三种：

(1) 穷举攻击

穷举攻击是一种暴力攻击的方式，采用穷举法遍历密钥空间，从而破解密码，过去对密钥空间小的系统十分有效，随着时代的发展，越来越多具有更大密钥空间的加密系统出现了，所以攻击者需要很长时间才能试出密钥，这会导致攻击失去实时性从而失效。

(2) 统计分析攻击

统计分析攻击从明文信息本身出发，运用统计分析方法分析其中的统计学规律，由于明文信息的相邻信息会存在一定的相关性，这些相关性可能会成为攻击者破密的有效武器。

(3) 数学分析攻击

数学分析攻击则是攻击者运用数学计算发现加解密规律，推出用以加密的算法，再采用其逆过程作为解密算法，破密得到有效的信息。

2.2.3 混沌图像加密经典结构

通常情况下，大部分混沌图像加密系统由置乱和扩散两部分组成，其结构如下所示。

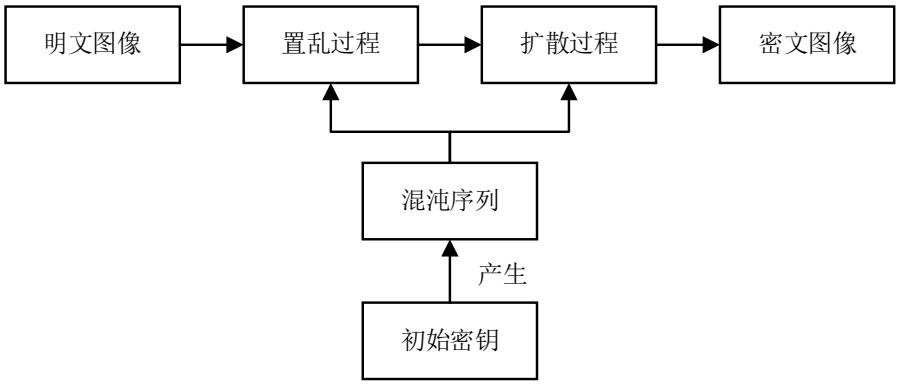


图 2.5 混沌图像加密算法的基本结构

一般地，置乱是将图像各像素点按一定的规则打乱顺序，打乱像素间的相关性。扩散是在像素之间进行一定规律的像素数值变换，而这种变换会使得图像与原图像的特征完全不一致。在计算能力范围内尽可能多地使用置乱和扩散会使加密效果更好。

第 3 章 基于级联混沌系统的图像加密算法

3.1 引言

目前，加密算法可分为两类。第一类包括经典的标准加密技术，如 AES、DES 和 RSA。这些算法适用于某些应用，如网络银行、互联网和网络安全。这些传统标准的主要不便之处在于，由于计算复杂，执行时间会变得很长。第二类包括使用香农混沌和扩散特性的算法。这些方法可以用于图像加密，因为它们结合了两个重要的标准：对几种攻击的鲁棒性和执行时间的增益。在这些方法中，当混沌映射被用于置乱和扩散阶段时，安全性会增加。

许多基于混沌和利用混沌特性的算法被研究者们提出[33-43]，以提高加密算法的复杂性和鲁棒性。这些方法中，置乱和扩散阶段使用的混沌映射是加密算法的核心。为此，人们提出了几种使用 1-D、2-D、3-D 和超混沌系统进行加密的方法。这些混沌系统之间最共同的一点是，如果初始条件或函数的参数稍有改变，就有可能给出不同的随机序列。因此，研究者们主张利用这一特性来构建算法的大密钥空间。然而，经典的映射，如 Logistic 映射、Tent 映射或 Sine 映射，只在很小的参数范围内能出现混沌。因此，有必要改进这些映射，以获得更好的混沌性能，同时保证较快的加密速度。

针对现有的问题，综合考虑各方面影响因素，本章提出了一种 1-D 和 2-D 级联的混沌映射，在不提升维度的情况下增加了系统的复杂度，并且整体来看，该系统在时间成本、运算成本、加密性能方面都优于其他的单个系统。

3.2 级联混沌系统简介

3.2.1 级联混沌系统结构及参数计算

由两个以上的混沌映射组合而成的系统被称为级联混沌系统(Cascade Chaotic System, CCS)，图 3.1 是 CCS 的结构，其中$G(x)$和$F(x)$是两个子映射。CCS 将两个子映射串联起来。将$G(x)$的输出输入到$F(x)$的输入中，然后将$F(x)$的输出反馈到$G(x)$的输入中进行递归迭代。

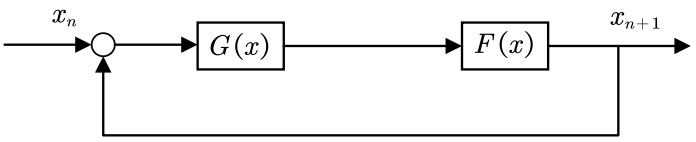


图 3.1 级联混沌系统 CCS 的结构

级联混沌系统的李亚普诺夫指数(Lyapunov Exponent, LE)计算：

(1) 假设x_0和y_0是 CCS 中的两个非常接近的初值，在第一次迭代后，差值$|x_1-y_1|$定义为：

$$\begin{aligned}|x_1-y_1| &= |\Gamma(x_0)-\Gamma(y_0)| \\ &= \frac{|F(G(x_0))-F(G(y_0))|}{|G(x_0)-G(y_0)|}\frac{|G(x_0)-G(y_0)|}{|x_0-y_0|}|x_0-y_0|\end{aligned} \tag{3.1}$$

(2) 我们可以得到：

$$\left|\frac{dF}{dx}|_{G(x_0)}\right| \approx \lim_{G(x_0)\to G(y_0)}\frac{|F(G(x_0))-F(G(y_0))|}{|G(x_0)-G(y_0)|} \tag{3.2}$$

$$\left|\frac{dG}{dx}|_{x_0}\right| \approx \lim_{x_0\to y_0}\frac{|G(x_0)-G(y_0)|}{|x_0-y_0|} \tag{3.3}$$

(3) 因此：

$$|x_1-y_1| \approx \left|\frac{dF}{dx}|_{G(x_0)}\right|\left|\frac{dG}{dx}|_{x_0}\right||x_0-y_0| \tag{3.4}$$

(4) 同理，第二次迭代后，差值定义为：

$$\begin{aligned}|x_2-y_2| &= |\Gamma(x_1)-\Gamma(y_1)| \\ &= \frac{|F(G(x_1))-F(G(y_1))|}{|G(x_1)-G(y_1)|}\frac{|G(x_1)-G(y_1)|}{|x_1-y_1|}|x_1-y_1| \\ &\approx \left|\frac{dF}{dx}|_{G(x_1)}\right|\left|\frac{dG}{dx}|_{x_1}\right|\left|\frac{dF}{dx}|_{G(x_0)}\right|\left|\frac{dG}{dx}|_{x_0}\right||x_0-y_0|\end{aligned} \tag{3.5}$$

(5) 经过$n(n\to\infty)$次迭代后，$|x_n-y_n|$定义为：

$$\begin{aligned}|x_n-y_n| &= |\Gamma(x_{n-1})-\Gamma(y_{n-1})| \\ &\approx \left|\prod_{i=0}^{n-1}\frac{dF}{dx}|_{G(x_i)}\right|\left|\prod_{i=0}^{n-1}\frac{dG}{dx}|_{x_i}\right||x_0-y_0|\end{aligned} \tag{3.6}$$

(6) 从$|x_0-y_0|$到$|x_n-y_n|$的迭代平均变化值为：

$$\Delta_{\Gamma(x)}\approx\left\{\left|\prod_{i=0}^{n-1}\frac{dF}{dx}|_{G(x_i)}\right|\left|\prod_{i=0}^{n-1}\frac{dG}{dx}|_{x_i}\right|\right\}^{\frac{1}{n}} \tag{3.7}$$

(7) 因此：

$$\lambda_{\Gamma(x)}=\ln(\Delta_{\Gamma(x)})=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\frac{dF}{dx}|_{G(x_i)}\right|+\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\frac{dG}{dx}|_{x_i}\right| \tag{3.8}$$

(8) $G(x)$和$F(x)$的 LE 值被定义为：

$$\lambda_{F(x)}=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\frac{dF}{dx}|_{G(x_i)}\right| \tag{3.9}$$

$$\lambda_{G(x)}=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\frac{dG}{dx}|_{x_i}\right| \tag{3.10}$$

(9) 所以，级联混沌系统的 LE 值为两个子系统的 LE 值之和：

$$\lambda_{\Gamma(x)}=\lambda_{F(x)}+\lambda_{G(x)} \tag{3.11}$$

当$\lambda_{\Gamma(x)}>0$时，随着迭代次数的增加，CCS 的两个输出序列轨迹变化剧烈，CCS 开始进入混沌状态，LE 的值越大，两条轨迹越分散，混沌性能越好。混沌性能总结如下：

① 当$\lambda_{F(x)}>0$，$\lambda_{G(x)}>0$时，有$\lambda_{\Gamma(x)}>0$，并且$\lambda_{\Gamma(x)}>\lambda_{F(x)},\lambda_{\Gamma(x)}>\lambda_{G(x)}$，两个子映射处于混沌状态，则 CCS 也处于混沌状态，比任何一个子映射的混沌性能都要好。

② 当$\lambda_{F(x)}<0$，$\lambda_{G(x)}<0$时，有$\lambda_{\Gamma(x)}<0$，CCS 不具有混沌特性。

③ 当$\lambda_{F(x)}>0$，$\lambda_{G(x)}<0$或者$\lambda_{F(x)}<0$，$\lambda_{G(x)}>0$时，我们有：

$$\lambda_{\Gamma(x)}\begin{cases}>0 & (\lambda_{F(x)}+\lambda_{G(x)}>0)\\ <0 & (\lambda_{F(x)}+\lambda_{G(x)}<0)\end{cases}$$

所以，经过数学证明可知，级联混沌系统会具有更好的混沌性能（当两个子映射都处于混沌状态）。

3.2.2 改进的 Henon-Sine 映射

经典的 1-D 混沌系统虽计算方便，但由于其密钥空间小，且混沌区间有限，不适合单独用于加密系统，因此，Y. Zhou 等人提出了 Tent-Logistic、Double-Sine

等多种级联混沌系统，并对其做了相关性测试[44]，性能较单个的 1-D 混沌系统有显著的改善，这些系统均由两个 1-D 混沌系统级联而成，具有更复杂的轨迹，输出结果也更加不可预测。在这之后，越来越多复杂的级联系统被提出，其中，Alawida 等人实验结果表明[45]，在允许的计算范围内，一个 1-D 混沌系统和一个 2-D 混沌系统级联的系统具有较好的混沌性能，他们采用了 Henon-Cosine 映射 (Cosine-based digital Henon Map, CHM)，该映射与一般的 Henon-Cosine 映射区别在于他们在 Cosine 函数内部添加了一个指数参数作为控制参数，从而增加系统的混沌复杂性，受得该研究启发，本文提出了一个改进的 Henon-Sine 映射 (Improved Sine-based digital Henon Map, ICSM)，相较于 CHM 的优势如下：

(1) ICSM 中，Henon 映射中的控制参数均成为了其指数项，经过绘制混沌分岔图并验证[46]，该映射具有更好的混沌性能。

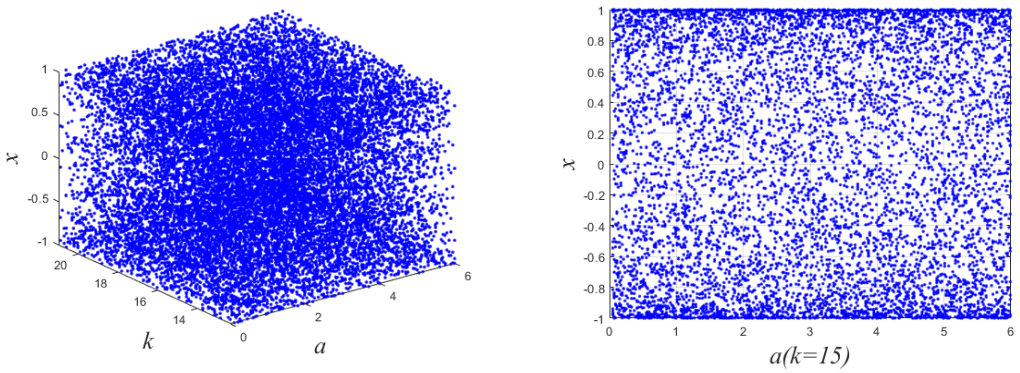
(2) ICSM 的 Lyapunov 指数均为正，接近于常见的超混沌系统，这说明其混沌性能较好，并且有着复杂的运动轨迹和非周期性。

(3) ICSM 的组成不算复杂，便于在软硬件上实现，由于该映射比超混沌系统的结构精简许多，是低维映射，适合用于像图像加密这种对快速性要求高的场合。

ICSM 的公式如下：

$$\begin{cases} x_{n+1} = \cos\left(2^{(k+(1-a\cos y_n - a\sin x_n))}\right) \\ y_{n+1} = \cos\left(2^{(k+x_n+b)}\right) \end{cases} \tag{3.12}$$

其中$a \in [1.5, 5], k \in [10, 24], b = 0.3$时，ICSM 是处于完全混沌状态的，相较于 CHM 映射有更好的遍历性和随机性，因此 ICSM 具有更复杂的轨迹且输出结果更加不可预测。



(a) (b)

图 3.2 (a) ICSM 的分岔图 (b) ICSM 的分岔图(k=15)

3.3 加密解密方案

3.3.1 混沌奇异变换 CMT

数字图像由于相邻像素之间的相关性较大，信息特征较为明显。通常采用随机改变图像像素位置的方法降低这些相关性来防御攻击者，因此，一种新的混沌奇异变换(Chaotic magic transform, CMT)被提出。

表 3.1 混沌奇异变换

输入：原始图像矩阵 P 和混沌矩阵 S（大小均为 $M \times N$）

1：使用 *sort* 函数对 S 的各列进行大小排序，得到排序结果 R

2：生成排序矩阵 I：$I(i,j)=k \quad \text{for } R(i,j)=S(k,j)$

3：**for** $i=1:M$ **do**

4: 将图像矩阵 P 的像 $(I_{i,1},1),(I_{i,2},2),\ldots,(I_{i,N},N)$ 连接成一个圆形队列

5: 对这些关联起来的像素串进行向右平移 i 个单位

6: **end for**

输出：加密图像 T

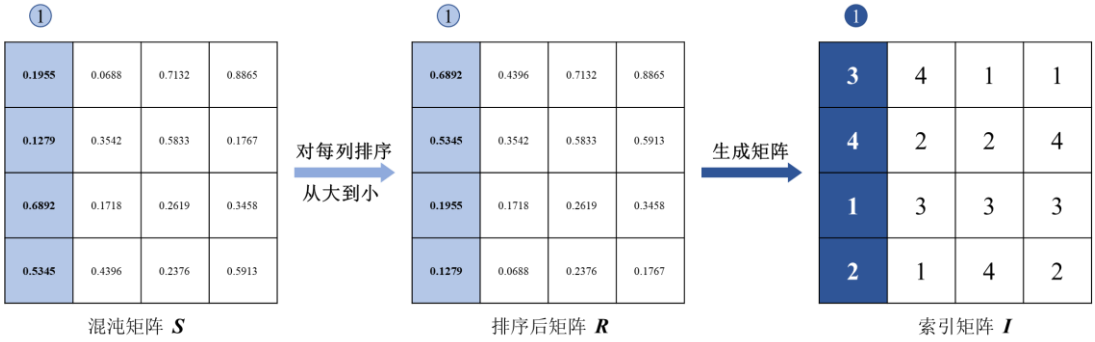
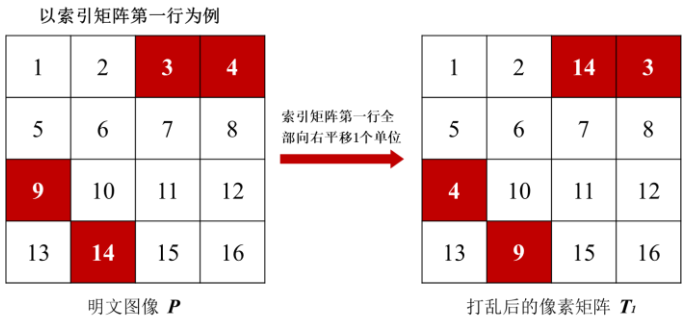


图 3.3 变换示意图



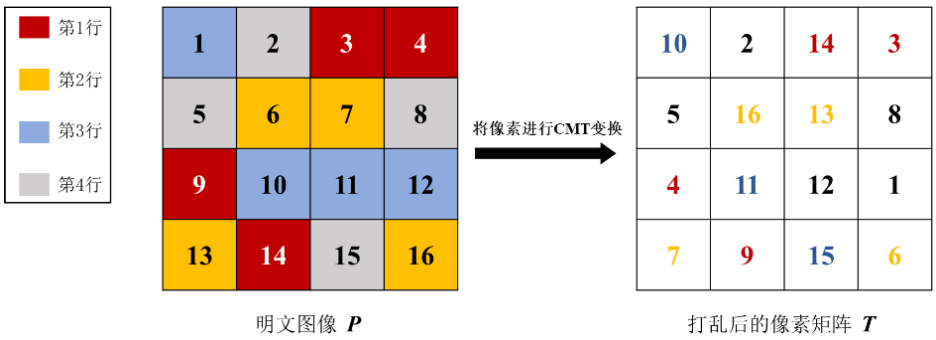


图 3.4 像素进行 CMT 变换的一个例子

上述图为 CMT 变换的示例。我们可以看到由排序混沌矩阵I的每一列降序排序，得到索引矩阵I。索引矩阵I表示R中数据的排列位置。在图中，P为原始图像矩阵，T为 CMT 的排序结果。由于索引矩阵I有 4 行，打乱过程可以分为如下几个步骤。首先以索引矩阵I第一行为例，如图 3.4 所示，我们将矩阵 P 中红色的部分$(P_{3,1},P_{4,2},P_{1,3},P_{1,4})$，即矩阵中的(4,9,14,3)连接成一个环形，随后将他们依次向右平移一个单位，结果为矩阵T_1中红色的部分。然后，将其余的部分进行 CMT 变换，如图 3.4 所示，每行的颜色都不同，打乱后可以发现像素与明文图像的像素已有很大的差别。最后，经过所有的运算操作，我们可以得到 CMT 的结果 T。CMT 的优点是可以将一个像素与其相邻像素快速分离，同时在不了解混沌映射的详细情况下，CMT 结果极难预测，安全性较高。

3.3.2 像素扩散

对于加密算法来说，具有良好扩散特性意味着具有抵抗选择明文攻击的能力。扩散特性表明，使用相同的安全密钥加密两个差别很小的明文，会产生完全不同的加密结果。为了获得良好的扩散特性，CMT-ICSM 分两步进行像素扩散:行扩散和列扩散。

假设明文图像经过 CMT 变换后的结果 T 和混沌矩阵 S 的大小都为$M\times N$，由如下数学式定义：

$$C_i=\begin{cases}(T_i+T_R+floor(S_i\times 2^{32}))\ mod\ F & i=1\\ (T_i+C_{i-1}+floor(S_i\times 2^{32}))\ mod\ F & i\in[2,R]\end{cases} \tag{3.13}$$

其中，F为明文图像中像素最大值，例如彩色图像通常$F=256$，当进行行扩散时，$R=N$并且上式用于T的每一行，当进行列扩散时，$R=M$并作用在T的每一列。

3.3.3 基于混沌奇异变换的图像加密算法

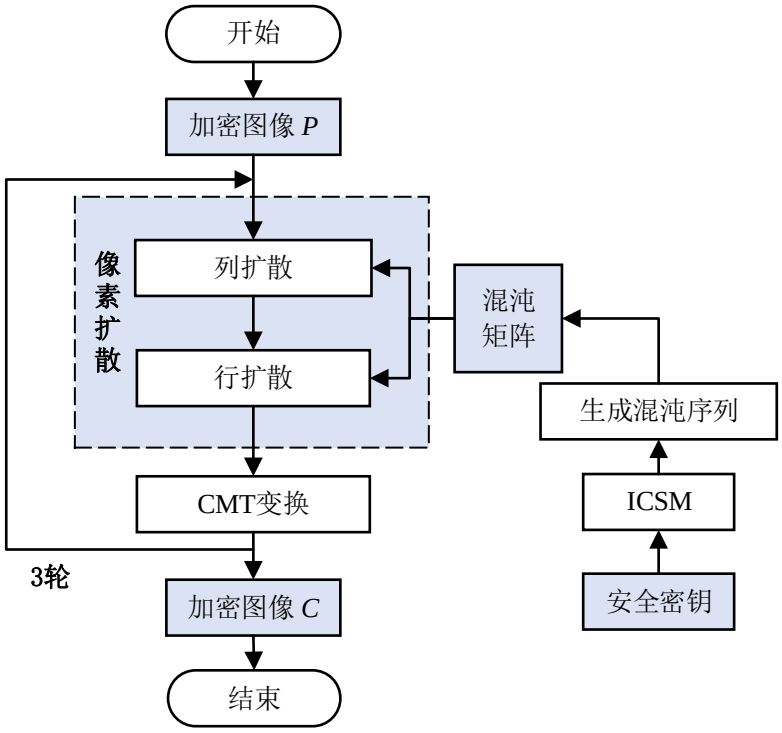


图 3.5 改进的 CMT 算法流程图

利用提出的 ICSM 和 CMT，本节提出了一种新的基于 CMT 的图像加密算法，称为 CMT-ICSM。利用 ICSM 生成伪随机序列，CMT 通过伪随机序列来改变图像像素位置，通过像素替换来改变图像像素值。

CMT-ICSM 的工作流程如图 3.5 所示。明文图像 *P* 是原始图像，密文图像 *C* 是加密图像。安全密钥用于生成 ICSM 的初始值和参数。CMT 是通过对所有像素位置进行随机打乱来实现混沌性能。像素扩散操作是通过随机改变所有像素值来获得扩散特性，获得类似随机的加密结果，同时避免 CMT-ICSM 在某些参数设置下，可能会失去其混沌性能，本文提出的 CMT-ICSM 采用了两轮 CMT 和像素替换操作。解密过程只是逆转了 CMT-ICSM 的加密操作。

以一个4×4的矩阵为例，经过算法加密后的结果如下图，可以看到结果与原矩阵完全不具有相似处。

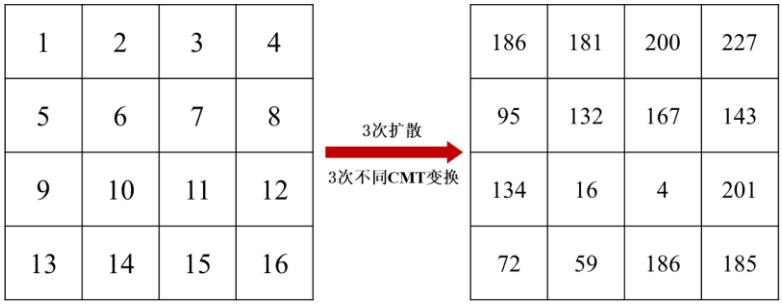


图 3.6 使用 CMT-ICSM 算法得到的结果

3.3.3 加密算法步骤

以大小为$M \times N$的数字图像P作为待加密图像，加密步骤如下所示：

(1) 生成初始条件

CMT-ICSM 的安全密钥是一个 256 位的序列。其结构如图所示。它包含了 ICSM 的初始值和参数信息，可分为 7 部分。

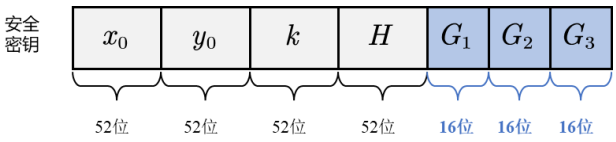


图 3.7 安全密钥的结构

其中前四个参数是由一段 52 位的字符串用 IEEE 754 格式生成的十进制数[47]

$$x = \frac{\sum_{i=1}^{52} b_i 2^{52-i}}{2^{52}} \tag{3.14}$$

后三个参数是由 16 位字符串产生的两个整数系数，用于生成两个混沌矩阵如下式所示。

$$\begin{cases} x_{0i} = (x_0 + G_i H) \ mod \ 1 \\ y_{0i} = (y_0 + G_i H) \ mod \ 1 \\ k_i = 12 + ((k + G_i H) \ mod \ 4) \end{cases} \tag{3.15}$$

其中，$i = 1, 2, 3$

在上式中，生成的初值范围在$[0, 1]$内，控制参数k_i会被限制在区间$[12, 16]$内，因此，在这些设置下，ICSM 会具有良好的混沌性能。

在提出的 CMT-ICSM 中，用户可以灵活地手动选择 256 位的二进制序列或随机生成二进制流来生成安全密钥。在本文的测试过程中，我们使用随机生成二进制的方法来生成密钥。

(2) 图像加密

将图像的像素值转为像素矩阵，依次经过 3 轮 CMT 变换和扩散后，得到加密后的像素矩阵，并将其用图片显示，我们用图像处理常用的一张图片 Cameraman 举例演示。

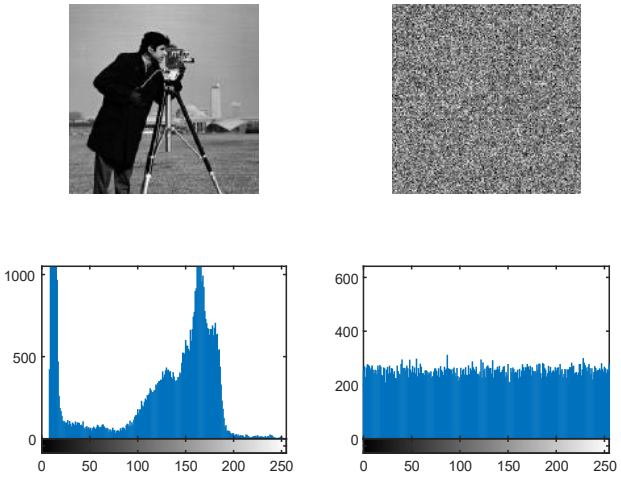


图 3.8 图像加密结果与图像的直方图

图 3.8 显示了经过使用图像加密算法后，像素矩阵变成了另一个随机分布的数据矩阵，图像变成了一个类似随机的图像。从直方图中我们可以观察到图中加密图像的分布情况，每个灰度级的像素数几乎相等。攻击者使用任何统计分析方法都难以获得原始图像的信息。同样，这种方法也可以用于其他的数据加密，如语音，文字等等。

3.3.4 解密步骤

解密过程即对加密后的图像进行与加密时完全相反的逆操作，且一定要用与加密时完全相同的密钥，最后得到的解密图像才会与明文图像一致。

3.4 仿真结果与安全性分析

3.4.1 仿真结果

在 Windows10 64 位系统，Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz, 8.00GB RAM 环境下运行 MATLAB R2021a 软件。使用本章提出的算法对 Cameraman.tif, Lena.tif, Baboon.tif, Peppers.tif, Goldhill.tif 的灰度图像进行加密和解密。

一个好的图像加密算法，应该具有将不同类型的明文图像转换为类似随机的

密文图像的能力。这里给出了几个 CMT-ICSM 的模拟结果。

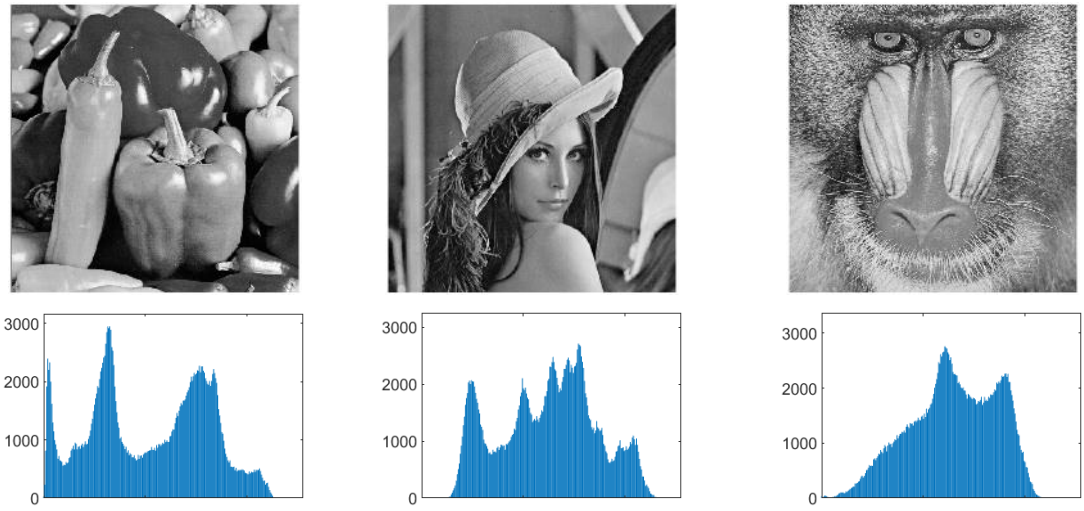


图 3.9(a) 加密前图像与直方图

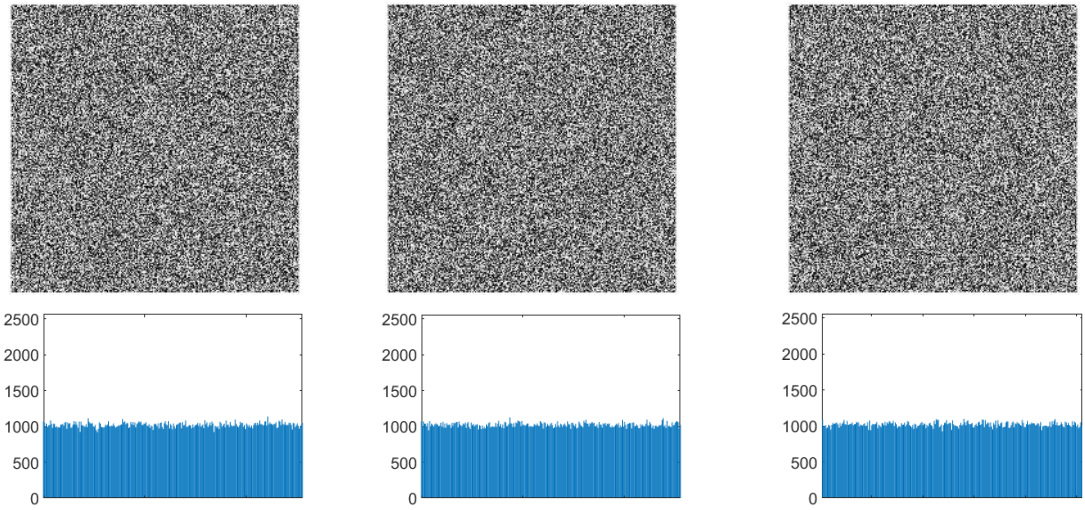


图 3.9(b) 加密后图像与直方图

图为 CMT-ICSM 对不同类型图像加密的模拟结果。仿真结果表明，本文提出的 CMT-ICSM 能够将全像素相同的图像转换为像素值随机均匀分布的类噪声加密图像，因此具有良好的加密性能。从图中可以看出，所有明文图像的直方图都是可以观察出图像的特征的；但密文图像都是随机的，很难从直方图中观察出有用的信息。它们不包含任何明文图像的信息。这表明 CMT-ICSM 对不同类型的图像具有良好的加密性能。

3.4.2 密钥空间分析

足够大的安全密钥空间是一个好的加密算法具有的特点，并且对其安全密钥的变化非常敏感。提出的 CMT-ICSM 密钥长度为 256 位，密钥空间为2^{256}。考虑当前计算机的计算能力，这足以抵抗穷举攻击。

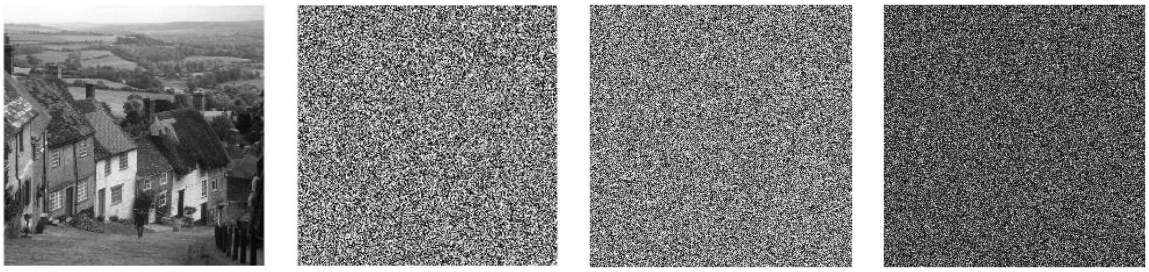
3.4.3 密钥敏感性分析

密钥的敏感性可以从两个方面来描述，

(1)安全密钥在加密过程中是十分敏感的。对一个明文图像进行加密，使用的是两个相差极小的加密密钥，但会得到的密文图像是完全不同的。

(2)安全密钥在解密过程中也是十分敏感的。若恢复一个密文图像，使用的是两个有微小差异的解密密钥，恢复出来的图像是完全不同的。

图 3-11 为关键敏感性分析结果。K2 和 K3 是由 K1 衍生而来的两个不同的秘钥，均只差一位。当使用 K1 和 K2 对明文图像进行加密时，加密结果完全不同。它们的差异如图 3-10(d)所示。



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

图 3.10 加密过程密钥敏感性分析: (a)原图 (b)K1 加密后 (c)K2 加密后 (d)K1 与 K2 加密后的差别（像素相减）

如图 3.11(b)所示，密文图像(图 3.11(a))只能由正确的密钥完全解密。当密文图像通过与 K1 相差一位的 K3 密钥解密时，解密结果也完全不同，无法识别。因此，提出的 CMT-ICSM 在加密和解密过程中都具有敏感性很高的安全密钥。

(a) (b) (c)

图 3.11 密钥敏感性分析: (a)K1 加密后的图像 (b)K1 解密后 (c)K3 解密后

3.4.4 差分攻击分析

差分攻击是一种在图像分析领域中较为普遍的攻击方法，该方法通过对原明文图像做些修改，再将其加密后，得到两张不同的加密图像，攻击者此时再试图

通过分析这图像的差别来得到明文图像和密文图像的联系。其中最重要的两个指标分别为两张加密图像之间的变化像素数(NPCR)和两张加密图像之间的平均变化强度数(UACI)，它们的理想值分别为 99.6094%和 33.4635%[48] ，计算公式如下：

$$NPCR=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}D(i,j)}{m\times n}\times 100\% \tag{3.16}$$

$$D(i,j)=\begin{cases}0, C_1(i,j)=C_2(i,j);\\ 1, C_1(i,j)\neq C_2(i,j);\end{cases} \tag{3.17}$$

$$UACI=\frac{1}{m\times n}\left(\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right)\times 100\% \tag{3.18}$$

表 3.2 NPCR 和 UACI 结果

图像	NPCR(%)	UACI(%)
Cameraman.tif	99.6277	33.4585
Lena.tif	99.6281	33.4783
Baboon.tif	99.5964	33.4800
Peppers.tif	99.5911	33.4765
Goldhill.tif	99.5903	33.4591

从表中数据可看到，得到的 NPCR 与 UACI 非常接近理想值，故该加密算法加密效果较好，能抵御差分攻击。

3.4.5 相邻像素相关性分析

通常情况下，一幅图像的像素与其相邻像素之间具有较高的相关性。图像防御攻击的能力与其相邻位置数据值的关联性呈反比关系，为了测试图像的抗攻击能力，分别随机选取图像在水平、垂直和对角线方向相邻的像素点进行分析。数据相关性由下式定义：

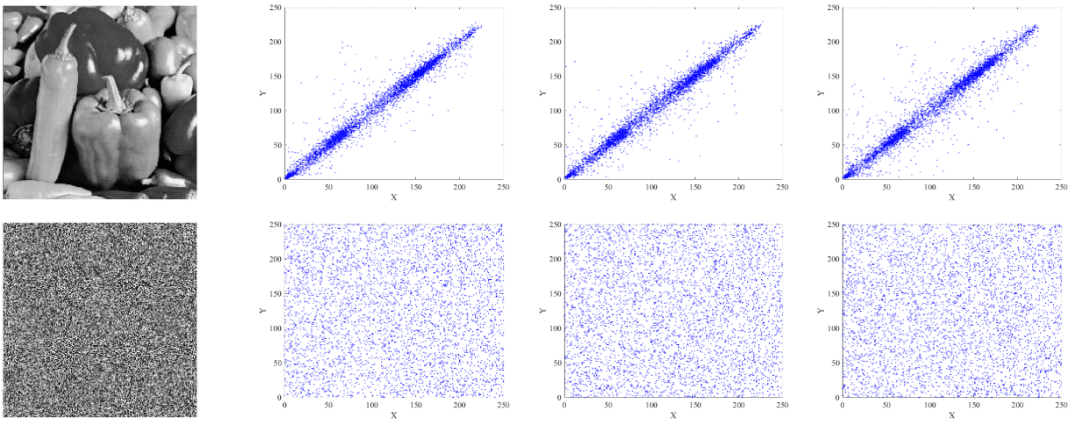
$$Corr=\frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma_X\sigma_Y} \tag{3.19}$$

其中X和Y是两个数据序列，μ是平均值，σ是标准差，如果X和Y具有较强的相关性，则相关性接近 1，否则接近于 0。

表 3.3 Peppers 图像及其加密图像的像素相关性

图像	水平	垂直	对角
原始图像	0.982856	0.979426	0.968485
加密图像	0.003554	0.006477	-0.001736

在我们的测试中，我们在水平、垂直和对角方向上随机选择 5000 个像素及其对应的相邻像素。下图给出了本文 CMT-ICSM 生成的明文图像及其密文图像的像素序列对，X,Y 的分布。结果显示，明文图像的大多数点位于坐标系对角线上或附近，而密文图像的所有点都是随机分布的。这意味着明文图像中相邻像素值相等或接近，而密文图像中相邻像素值变化很大。相邻像素相关检验的结果表明，明文图像的结果为强相关，密文图像的结果基本不相关。这进一步验证了 CMT-ICSM 加密后的图像相关性极低。



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

图 3.12 (a)明文图像、密文图像在 (b)水平方向 (c)垂直方向
(d)对角线方向相邻像素序列对的分布

3.4.6 信息熵

与直方图分析给出的直观结果显示图像像素均匀分布不同，局部香农熵 (Local Shannon Entropy, LSE)[49-50]，也称信息熵，是一个定性标准，用以评估图像的随机性。由下式定义：

$$H(k) = -\sum_{i=0}^{L-1} P(k_i)\log_2 P(k_i) \tag{3.20}$$

其中L是灰度级层次，$P(k_i)$是信息发生的概率，若存在所有像素灰度级概率都近似的随机图像，由上式计算出信息熵的理想值，如果越接近理想值，则加密后图像的的不确定性和随机性更高，这也表征了加密算法的不确定性和随机性。

表 3.4 信息熵分析结果

图像	尺寸	原图信息熵	加密后信息熵
Cameraman.tif	256*256	5.7847	7.9032
Lena.tif	512*512	6.0209	7.9061
Baboon.tif	512*512	7.0524	7.9025
Peppers.tif	512*512	6.4492	7.9046
Goldhill.tif	512*512	5.9270	7.9016

3.4.7 抗裁剪攻击分析

当密文图像受到裁剪攻击时，仍需要解密后的图像信息具有可读性，而这就要求我们的算法能将受损的密文图像最大限度上复原成明文图像，选用 Peppers.tif 进行抗裁剪攻击分析实验，结果如下图所示。

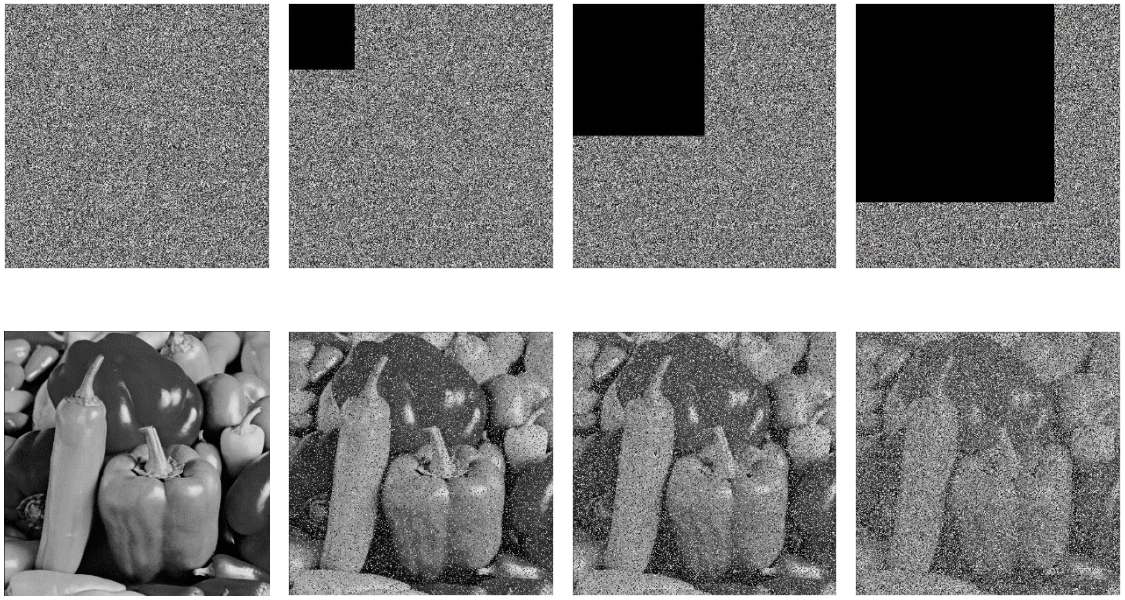


图 3.13 裁剪攻击分析

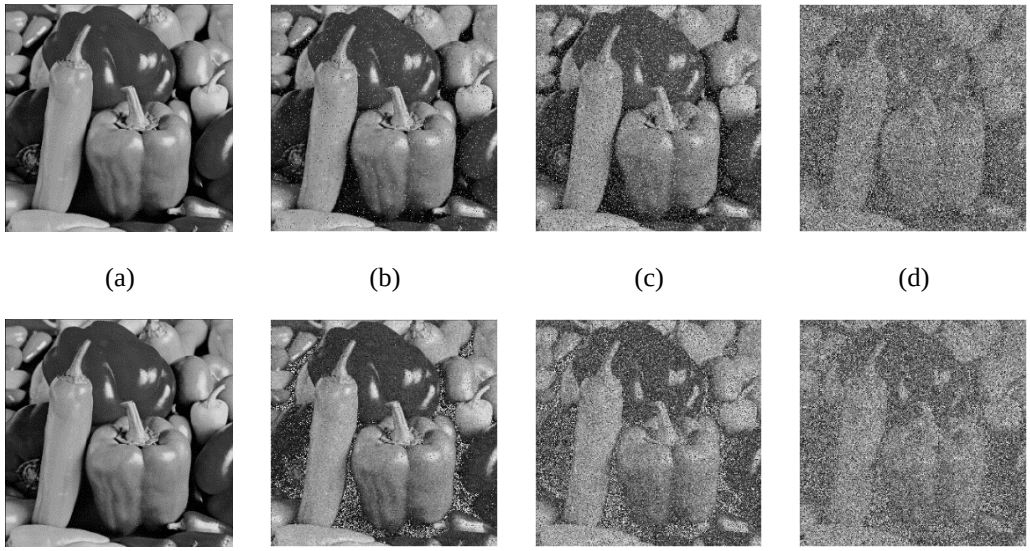
此图像上包含了诸多细节信息，对此图像进行加密，再对加密后的密文图像部分裁剪破坏，最后观察此密文图像解密后的结果。

由结果可以观察到，即便图像密文的部分被裁剪攻击破坏，导致密文部分的信息丢失，但是本章所提出的算法仍然很好地将图像复现了出来，并且将此攻击作用在图像上的影响均匀地分布在了整个图像上，使得图像具有很好的可读性，这表明该算法的抗裁剪攻击性能强。

3.4.8 抗噪声攻击分析

当数字图像通过网络传输或存储在物理媒体上时，数据丢失很容易产生，这是由于受到噪声的污染。因此，较强的抗噪声和数据丢失的鲁棒性是一个图像加密算法应该具有的，在本文提出的 CMT-ICSM 中，加密和解密过程是不对称的。

在加密过程中，密文图像中的所有像素会被明文图像中的一个像素变化而扩散到。然而，在解密过程中，一个像素的变化只会影响恢复结果中的少数像素。因此，CMT-ICSM 能够对带有噪声或数据丢失的密文图像进行解密。下图为 CMT-ICSM 对噪声和数据丢失的鲁棒性分析结果。可以看出，当密文图像在受到椒盐噪声和高斯噪声干扰时，CMT-ICSM 的解密过程仍然可以恢复原始图像。虽然恢复后的图像带有一些噪声，但我们仍然可以识别出大部分图像信息。



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

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

图 3.14 噪声攻击分析

(a)原图 (b-d)椒盐噪声攻击 密度 0.01/0.1/0.2

(e)原图 (f-h)高斯噪声攻击 方差 0.0001/0.0005/0.001

3.5 本章小结

本章的创新点在于，设计了一种基于级联混沌系统的图像加密算法，首先提出了一种新的级联混沌系统——ICSM。它是由 Sine 和 Henon 映射导出的。采用轨迹、Lyapunov 指数等评价方法对 ICSM 的混沌性能进行了评价。分析和评价结果表明，ICSM 比现有的大多数混沌映射具有更好的混沌性能。另外，本文引入了混沌奇异变换(CMT) 用以展示 ICSM 在图像加密中的表现。大量的实验结果表明，该算法对不同的图像都具有较高的安全性和较强的抗干扰性。

第 4 章 图像加密系统 GUI 设计功能与实现

本文图像加密系统虽然在理论上被验证是可行的，但也需将其应用到实际中，为了减少重复地操作，本章设计了一款图像加密的 GUI，实现了加密图像、解密图像，显示直方图、显示像素相关性等安全性分析，并将生成的密钥保存下来，可对不同的用户提供不同固定的密钥，较好地提升了研究效率。

4.1 总体设计

该系统主要由三个部分组成，分别是：加密图像、图像解密、安全性分析，安全性分析可添加许多指标分析，但由于界面大小有限，故这些指标被暂存在 MATLAB 工作区，需要的时候可以很方便的查看这些值，并且当系统被更换时，只需在程序内部更换算法与 GUI 的接口，即可实现更换图像加密系统，十分方便，此外，该 GUI 也设置了打开与退出功能，当每执行一次操作时，系统会发出提示信息，极大程度上提升了用户的体验。加密系统的主要流程如下所示。

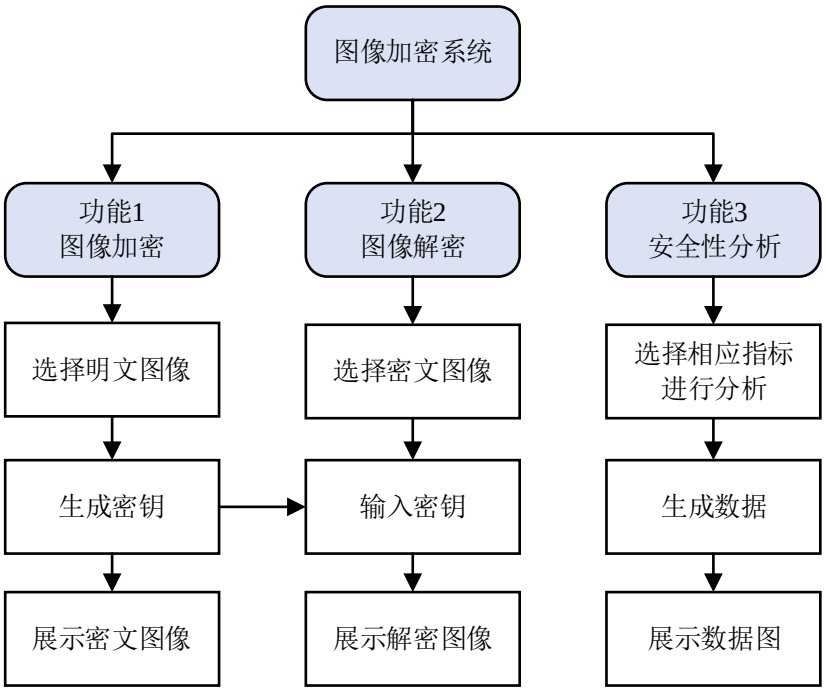


图 4.1 加密系统功能图

4.2 GUI 设计与功能实现

使用 MATLAB R2021a 中的 APP Designer 工具箱制作而成，该界面虽然简洁，但是可实现基本的功能，后期会对界面进行完善与美化，如用 QT 软件制作界面，令用户使用起来体验更好。

图 4.2 加密系统界面

其中，顶部的菜单栏共有四个选项，文件选项包含了子选项：打开图片、退出，打开图片是用户必须执行的一项操作，如果不执行该操作，则系统会发出消息框提醒用户加载图片，如图所示。

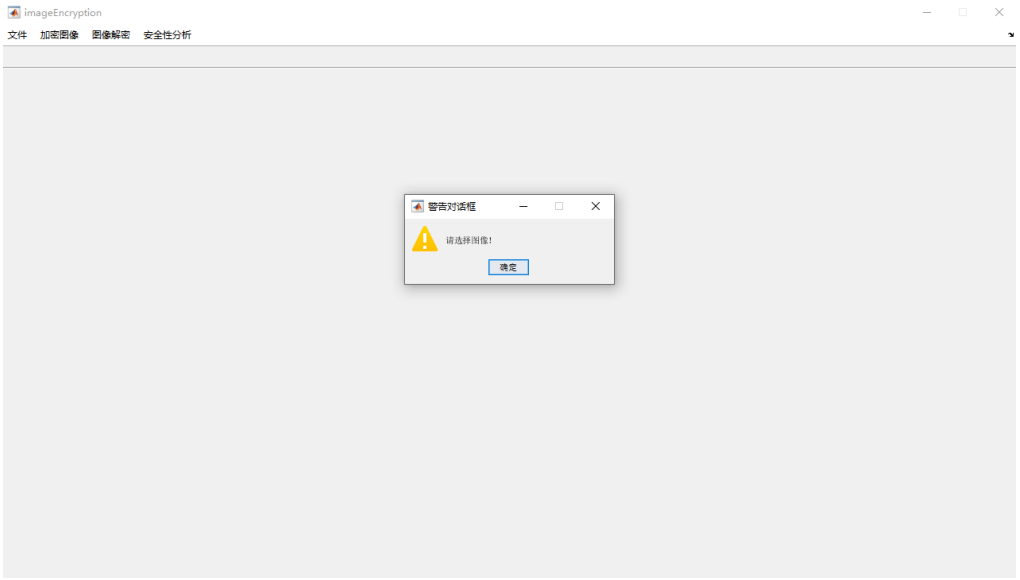


图 4.3 提醒消息框

加密图像按钮则是会调用图像加密算法 m 文件(ImageCipher.m)，对选择图像进行加密，并将密钥 K 以 mat 格式自动存储在当前文件夹，方便用户记录、查询密钥，加密完成后，被加密的图像将显示在界面上，图像的直方图也会随之生成，十分直观。

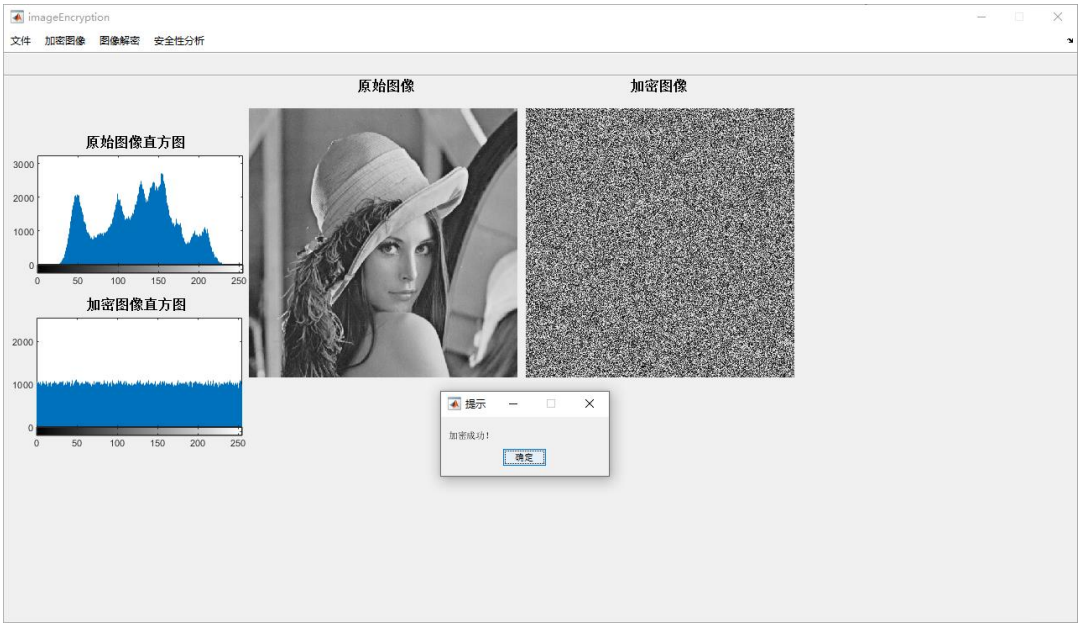


图 4.4 加密图像结果

解密图像按钮同样会调用解密算法文件，本文的加解密算法在同一个文件里，只需在 GUI 文件中加载指定的密钥，即可对图像解密成功，同时在界面中会出现被解密的图像与直方图，如下图所示。

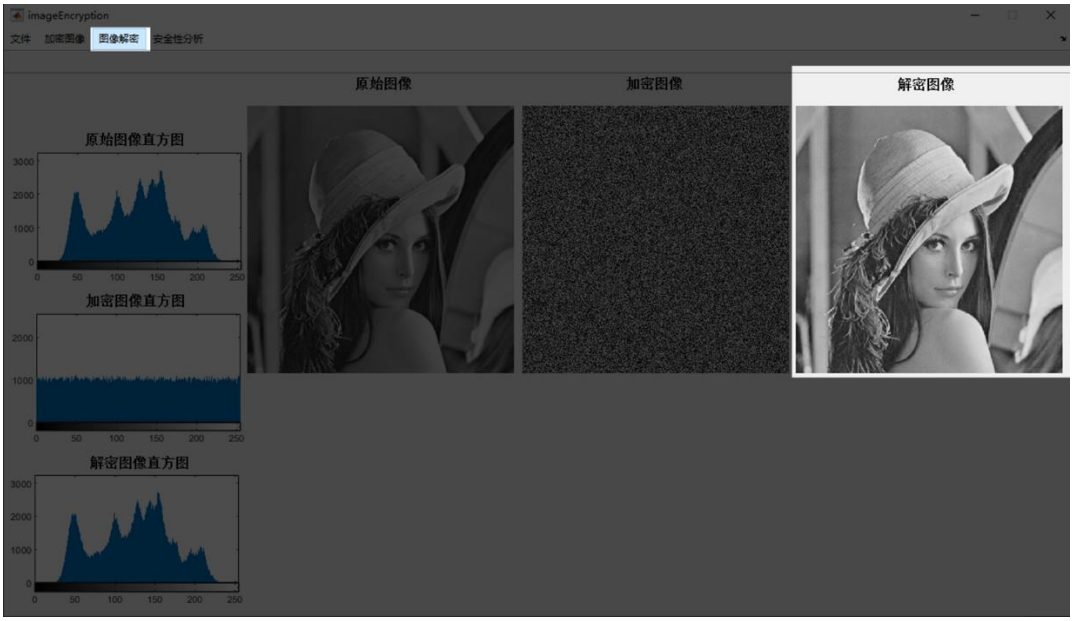


图 4.5 解密图像结果

最后一项功能是安全性分析，这里为了方便演示，只选取了像素相关性分析呈现在界面上，点击安全性分析中的像素相关性，即可生成三幅像素相关性的图片，如下图所示。

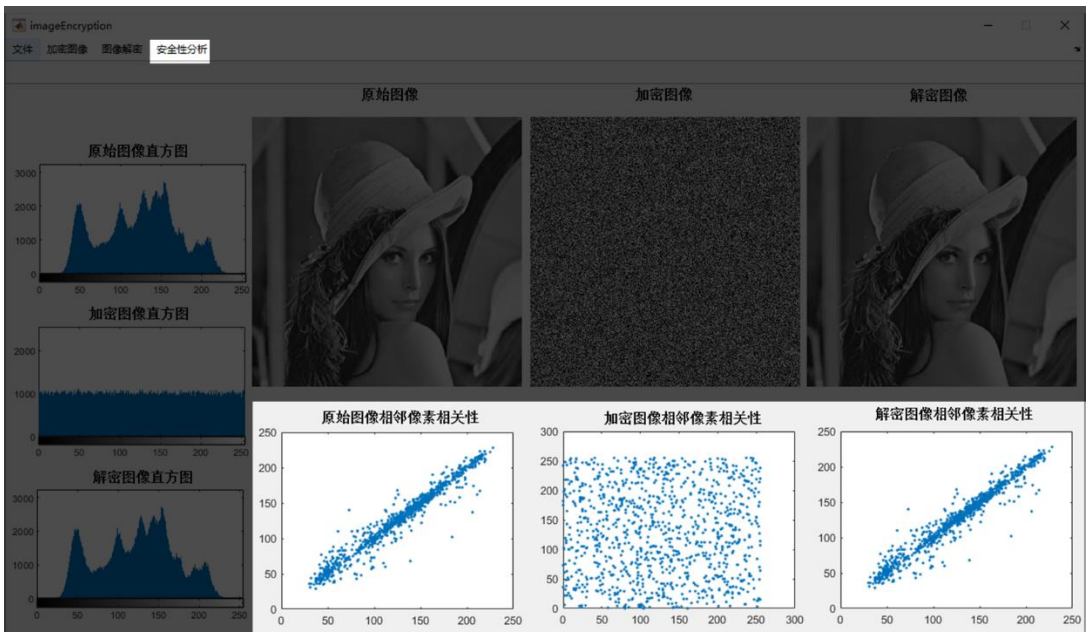

imageEncryption
文件
加密图像
图像解密
安全性分析
原始图像
加密图像
解密图像
原始图像直方图
加密图像直方图
解密图像直方图
原始图像相邻像素相关性
加密图像相邻像素相关性
解密图像相邻像素相关性

图 4.6 安全性分析结果

第 5 章 总结与展望

5.1 总结

伴随着快速发展的网络通信和大数据应用，一个非常重要的热点问题之一是信息安全，而数据加密是保护信息安全最有效的方法。混沌具有的这些特殊性质，使得混沌十分适合用于图像加密，数字图像与文本信息、语音信息相比，在传输信息方面更为有效，现如今聊天软件的功能越来越多，传输图片方面已出现了其他功能，如闪照等，而闪照作为一种保护数字图像的方式，采用的方法就是简单的图像加密，而伴随着人们对图像安全的重视程度日益提高，在图像安全方面也需要有相应方法来满足人们的需要，以保障人们的生活安全。另外，图像安全一个更重要的应用是在军事领域，在军事作战中最重要的就是数据的传输，敌军常常会用一系列手段和方式干扰我方的信息传输，以切断前线和指挥部的联系，而此时一个性能好的，抗干扰性强的信息加密方法重要性不言而喻。

在当今社会对安全性信息传输要求高的这种环境下，本文以混沌图像算法的安全分析与设计为核心内容，经过提出 Sine-Henon 映射，混沌奇异变换 CMT，以及相关的扩散、置乱算法，针对现有的社会背景进行分析，设计了一套混沌图像算法加密系统，并在最后试图将其运用到实际生活中。本文主要工作如下：

（1）介绍了混沌的基本理论、混沌的发展历程、以及解释在混沌图像加密中常见的名词，同时也介绍了几种常用于图像加密领域的混沌映射。

（2）提出了一种基于级联混沌系统的图像加密算法，对于现有大多数低维混沌系统性能低，高维混沌系统成本高的问题，首先提出了一种新的级联混沌系统——ICSM。它是由 Sine 和 Henon 映射导出的。采用像素相关性指数、噪声攻击等分析方法对 ICSM 的混沌性能进行了安全性分析。分析结果表明，该系统比现有的大多数混沌映射具有更好的混沌性能。另外，本文引入了混沌奇异变换(CMT)，这是一种较为创新的置乱方法，他的置乱结果只与混沌矩阵有关，而由于混沌的不可预测性，每次的加密结果都是不一样的，它可以快速地将图像中相邻的像素无需打乱。利用 ICSM 和 CMT，一种新的图像加密算法被提出，并且该算法具有较高的安全性和较强的抗干扰性。

（3）基于 MATLAB R2021a 的 APP Designer 工具箱，设计了一款混沌图像加密的 GUI，并且所含功能可基本满足普通用户的需求，同时也为研究图像加密的工作者们提供了一个较为方便的工具，省去了大量重复加密解密的时间，极大程度上提高了科研人员的工作效率。

5.2 展望

本文研究了混沌图像加密系统，虽然文中提出的算法，性能比一般的混沌加密系统强，安全性也较好，但是加密算法方面仍存在一些不足的地方，改进之后该算法应用在实际的可能性也会大大提高，因此，本文作者展望了混沌图像加密算法的研究方向，分为以下几点：

（1）在生成混沌映射的参数中采用了 IEEE 754 格式生成密钥，但是在网络安全方面，密钥的传输也同样是一个复杂的问题，如何安全地将密钥和信息传输至对方，并不被第三方窃取，这也是需要去研究的。

（2）近年来，随着手机的性能与存储量越来越大，我们在日常社交，网页浏览中加载的图像数据大大增加，再加上男女老少都拍照群体增多，人们对图像的数据质量需求也增加不少，过去的照片可能只有几百 K，而如今的一张高清照片可达几 M 甚至是几十 M。这对加密算法带来了严峻的考验，若在图像加密的过程中掺杂图像压缩技术，则可以大大提高用户体验，满足其对实时性要求高的需求。

（3）本文提出的算法只涉及像素矩阵上的数学操作，仍存在一定地规律，若结合当下热门的神经网络，机器学习领域设计一款可以自主学习的算法，自适应地调整混沌系统的参数，使之完全无迹可寻，这也同样具有一定的研究意义，可以在安全性要求更高的场合使用。

参考文献

[1] 郭宁. 基于混合差分隐私的流数据频数统计算法研究[D]. 哈尔滨工业大学硕士论文, 2019.

[2] 罗蒸. 基于多混沌系统的图像算法加密研究[D]. 重庆邮电大学硕士论文, 2021.

[3] 李春虎. 基于混沌的图像加密关键技术研究[D]. 电子科技大学硕士论文, 2018.

[4] 陈裕城. 混沌图像加密算法的分析与设计研究[D]. 广州大学博士论文, 2021.

[5] Elabady N F, Abdalkader H M, Moussa M I, Sabbeh S F. Image encryption based on new one-dimensional chaotic map. In Engineering and Technology (ICET), 2014 International Conference on (pp. 1-6). IEEE.

[6] Liu L, Miao S. A new simple one-dimensional chaotic map and its application for image encryption[J]. Multimedia Tools and Applications, 2018, 77(16): 21445-21462.

[7] Song C Y, Qiao Y L, Zhang X Z. An image encryption scheme based on new spatiotemporal chaos[J]. Optik-International Journal for Light and Electron Optics, 2013, 124(18): 3329-3334.

[8] 柴绍杰, 张彩珍. AES 加密算法的改进及 FPGA 实现[J]. 兰州交通大学学报, 2020,39(03):47-53.

[9] Farah M A, Farah A, Farah T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box[J]. Nonlinear Dynamics, 2020, 99(4): 3041-3064.

[10] 杜瑾. 基于混沌系统的无损图像加密算法[D]. 南昌大学硕士论文, 2021.

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

[12] Zhang Y Q, Wang X Y. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice[J]. Information Sciences, 2014, 273: 329-351.

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

[14] Hilborn R C. Chaos and nonlinear dynamics: an introduction for scientists and engineers[M]. Oxford University Press on Demand, 2000.

[15] Xiao F W, Song G S. A general efficient method for chaotic signal estimation[J]. IEEE Transactions on signal processing, 1999, 47(5): 1424-1428.

[16] Arroyo D, Rhouma R, Alvarez G, et al. On the security of a new image encryption scheme based on chaotic map lattices[J]. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2008, 18(3): 033112.

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

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

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

[20] Boubaker O, Jafary S. Recent advances in chaotic systems and synchronization: from theory to real world applications[J]. 2018.

[21] Abdul M M, Mohammed A N. Review on Chaotic Theory using DNA Encoding with Image Encryption[J]. Informatica: Journal of Applied Machines Electrical Electronics Computer Science and Communication Systems, 2021, 2(1): 14-19.

[22] Moon S, Baik J J, Seo J M. Chaos synchronization in generalized Lorenz systems and an application to image encryption[J]. Communications in Nonlinear Science and Numerical Simulation, 2021, 96: 105708.

[23] Shirazi F A Z, Hakimi E, Hosseini A, et al. Li-Yorke and Devaney chaotic uniform dynamical systems amongst weighted shifts[J]. arXiv e-prints:2204.07950, 2022.

[24] 雷宇航. 基于同时置乱和扩散操作的快速混沌图像加密方案研究[D]. 长安大学硕士论文, 2021.

[25] 张磊. 基于混沌的多图像加密算法研究[D]. 中国矿业大学硕士论文, 2021.

[26] 刘倩. 基于混沌映射的图像加密算法研究[D]. 南昌大学硕士论文, 2020.

[27] 朱金玉. 基于二维混沌映射的图像加密算法研究[D]. 桂林电子科技大学硕士论文, 2021.

[28] 杜瑾. 基于混沌系统的无损图像加密算法[D]. 南昌大学硕士论文, 2021.

[29] 蒋刚. 基于混沌的数字图像加密算法设计与仿真[D]. 贵州大学硕士论文, 2021.

[30] Cao J, Chugh R. Chaotic behavior of logistic map in superior orbit and an improved chaos-based traffic control model[J]. Nonlinear Dynamics, 2018, 94(2): 959-975.

[31] 王勇, 杨锦, 王瑛. 改进 Henon 超混沌系统与 AES 结合的图像加密算法[J]. 计算机工程与应用, 2019, 55(22): 180-186.

[32] Wang Z, Lou Y, Wang W, et al. Research on the application of LDPC code in chaotic sequence image encryption[J]. Cluster Computing, 2019, 22(3): 6359-6370.

[33] Lu Q, Zhu C, Deng X. An efficient image encryption scheme based on the LSS chaotic map and single S-box[J]. IEEE Access, 2020, 8: 25664-25678.

[34] Chen J, Chen L, Zhou Y. Cryptanalysis of a DNA-based image encryption scheme[J]. Information Sciences, 2020, 520: 130-141.

[35] Hua Z, Wang Y, Zhou Y. Image cipher using a new interactive two-dimensional chaotic map[C]. 2015 IEEE International Conference on Systems, Man, and Cybernetics. IEEE, 2015: 1804-1808.

[36] Lan R, He J, Wang S, et al. Integrated chaotic systems for image encryption[J]. Signal Processing, 2018, 147: 133-145.

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

[38] Artiles J A P, Chaves D P B, Pimentel C. Image encryption using block cipher and chaotic sequences[J]. Signal processing: image communication, 2019, 79: 24-31.

[39] 陈虹, 赵菊芳, 郭鹏飞, 黄洁, 肖成龙, 周沫, 侯宇婷. 基于混沌映射的分块循环 DNA 图像加密算法[J]. 计算机应用研究: 1-8 [2022-05-16].

[40] 徐浙君, 陈善雄. 基于卷积神经网络的混沌序列图像加密算法研究[J]. 科技通报, 2021, 37(10): 48-53+58.

[41] 李春彪, 赵云楠, 李雅宁, 孔思晓. 基于正弦反馈 Logistic 混沌映射的图像加密算法及其 FPGA 实现[J]. 电子与信息学报, 2021, 43(12): 3766-3774.

[42] 周红亮, 刘洪娟. 结合 DNA 编码的快速混沌图像加密算法[J]. 东北大学学报(自然科学版), 2021, 42(10): 1391-1399.

[43] 葛滨, 陈旭, 陈刚. 向量运算加速的超混沌图像加密算法[J]. 西安电子科技大学学报, 2021, 48(06): 187-196.

[44] Zhou Y, Hua Z, Pun C M, et al. Cascade chaotic system with applications[J]. IEEE transactions on cybernetics, 2014, 45(9): 2001-2012.

[45] Alawida M, Samsudin A, Teh J S. Digital cosine chaotic map for cryptographic applications[J]. IEEE Access, 2019, 7: 150609-150622.

[46] 张秋余, 宋宇杰. 基于改进 Henon 映射和超混沌的双重语音加密算法[J]. 电信科学, 2021, 37(12): 11-24.

[47] Wikipedia, Double-precision Floating-point Format – Wikipedia, the Free Encyclopedia, 2013 (online; accessed 10.12.13).

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

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

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

致谢

时光荏苒如白驹过隙，转眼间，四年已至，我在花椒求学的这段时光即将结束，回首过往，所经历的一切都犹如昨日发生，高考失利后的挫败，初入学校的紧张与好奇，学习的热情、第一次参加比赛的激情、面临推免的焦虑、被海外学校录取时的兴奋，还有意外收获的爱情。“不逼自己一把，永远不知道自己有多优秀”这句话一直激励着我。过往皆序章，未来皆可盼，同时也谨向一路以来给予我帮助与关怀的人致以最真诚的感谢。

首先，我要感谢我的实验室导师杨云老师，从大一下学期开始，我便留在电子创新基地度过了一个又一个寒暑假，从什么都不会的小白，到成为大创项目负责人，参加三大赛取得奖项，参加各类学科竞赛获得好成绩，一路以来，杨老师始终都给予了我支持与帮助，在面对各种困难时，我心态容易浮躁、慌张，是杨老师给予我建议，让我有底气去沉着冷静面对它们，越过一个又一个坎。从杨老师身上，我不仅学习了如何发现并解决问题的方法，还学习了许多为人处世的道理。非常感谢杨老师一直以来对我的悉心教导。

感谢我的毕设指导老师赖强老师，赖强老师在混沌领域有很高的学术造诣，学术成果颇丰，在做毕设的过程中，赖老师在学术上给予了我很大的帮助，让我能很快地找到我的研究方向，少走了很多弯路，同时也从赖老师自己对科研的感悟中学到了许多，对于论文的撰写，老师对我提了很多建议，老师的指导让我在论文写作方面的能力有了很大的提升，非常感谢赖老师的指导与教诲。

同时，感谢华东交通大学电气与自动化工程学院的老师们，认真为我们上好每一堂课，为我们提供学习指导以及良好的学习环境。

感谢我的父母一直在我求学道路上默默地奉献，尽管家庭条件非常的普通，但是父母仍无条件地支持我做的决定，支持我去留学，我会努力成长成为一个对社会有用的人，不辜负父母的期望。

其次，感谢我的班级、实验室的同学们。感谢朱强、陈佳乐等同学一直以来愿意和我一起参加数学建模比赛；感谢张秀敏、王子烨、闫雪晖等同学和我一次又一次合作参加互联网+、挑战杯、创青春竞赛，让我从一个内向的人变为敢于站在几百人面前演讲的人；感谢张泽毅、刘俊睿等同学，对我生活上的帮助。感谢你们一直以来的陪伴，愿你们前程似锦！

最后，感谢评阅本学位论文专家评委导师们。

攻读学位期间取得的成果

参与科研项目

[1] 基于 FAIMM 算法的多雷达组合重构 3-D 道路环境的研究.已结题.2020-2021（国家级大学生创新创业训练计划项目，负责人）

竞赛获奖

国家级：

[1] 全国大学生英语竞赛.三等奖.2019
[2] 美国大学生数学建模竞赛.H 奖(二等奖).2021
[3] 全国大学生电工数学建模竞赛.三等奖.2021
[4] 中青杯全国大学生数学建模竞赛.三等奖.2021
[5] 全国大学生英语竞赛.一等奖.2021
[6] 美国大学生数学建模竞赛.F 奖(特等奖提名奖).2022

省级：

[1] 第十二届“挑战杯”江西省大学生创业大赛.银奖.2020
[2] 全国大学生数学建模竞赛.省二等奖.2020
[3] 全国大学生电子设计竞赛.省二等奖.2020
[4] 第十七届“挑战杯”江西省大学生课外学术科技作品竞赛.三等奖.2021
[5] 第七届江西省“互联网+”大学生创新创业大赛.铜奖.2021
[6] 全国大学生数学建模竞赛.省三等奖.2021

个人荣誉

[1] 饶怀远.学业奖学金.校级.三等奖.2019
[2] 饶怀远.三好学生.校级.2019
[3] 饶怀远.学业奖学金.校级.一等奖.2020
[4] 饶怀远.三好学生.校级.2020
[5] 饶怀远.中车株机奖学金.校级.三等奖.2020
[6] 饶怀远.电气学院科技之星.校级.2020
[7] 饶怀远.学业奖学金.校级.一等奖.2021
[8] 饶怀远.三好学生.校级.2021
[9] 饶怀远.国家奖学金.国家级.2021