作品类别：☑软件设计 □硬件制作 □工程实践

密码学单人作品

题目：混沌置乱的循环阶分析

黄柏熙　PB23071429

基本信息表
作品题目：示例题目
作品类别：☑软件设计 □硬件制作 □工程实践
作品内容摘要： 量化评估 Logistic、Cubic 和 Sine 混沌映射构造置乱的循环特性：循环圈长度、每种长度的循环圈个数和总的循环阶，使用的方法为统计计算平均阶-N 曲线
关键词： 混沌置乱、循环阶、Logistic 映射、Cubic 映射、Sine 映射

目录

1 作品概述

1.1 引言

网络已经成为人们沟通交流的主要平台，但是网络为我们的沟通交流提供了极大的便捷的同时，也存在许多信息安全的相关问题，特别是信息的传递，对信息加密可以在一定的程度上保护信息的隐秘性，因此信息的加密是一项很值得研究的课题，本文评估了三种混沌映射：Logistic 映射、Cubic 映射和 Sine 映射的置乱效果

1.2 研究背景与意义

随着数据化时代的到来，数据泄露、恶意攻击的问题日益突出，信息安全的重要性在不断增长。

1975 年，美国数学家约克和美籍华人李天岩发表了《周期 3 意味着混沌》的文章，首次提出了“混沌”一词，阐述了混沌的数学定义，对混沌学的发展具有重大意义。自此以后，混沌研究开始蓬勃发展。

混沌是指在确定性动力学系统中，由于对初值敏感而表现出的类似随机的、不可预测的运动。混沌是确定的非线性系统中出现的内在随机性现象，其变化并非随机确貌似随机。[1]

混沌映射被用于生成混沌序列，这是一种由简单的确定性系统产生的随机性序列。一般混沌序列具有以下主要特征：

1. 随机性
2. 非线性
3. 对初值敏感依赖
4. 遍历性
5. 长期不可预测性

等等，混沌映射有时也可以当作随机数生成器。本文利用混沌映射进行置乱，可以在图像、视频、通讯等领域应用，以保护隐私数据

2 设计实现与方案

2.1 实验原理

利用混沌映射的随机性，将获得的 N 个数进行排序后，这 N 个数的下标也呈现随机性，再进行一步变换后达到置乱的效果。

循环圈长度越长，需要进行的置乱越多，更难回复原始数据，安全性更强；循环圈个数越多，可能意味着局部性越强 (短循环越多)，安全性可能下降；总循环长度越高，安全性越强，因为总循环长度反映的是最少需要多少次置乱才能恢复成初始状态。

2.2 构造置乱算法

1. 选定一个混沌映射
2. 选定参数 μ 和初始值 (即种子)x_0，迭代 M 轮得到 x_M，继续迭代计算 $x_{M+1} \sim x_{M+N}$
3. 将这 N 个数按照大小排序，以每个数的位置为置乱索引。例如，x_i 被排在第 j，位，则置乱中将第 i 个数移至第 j 位

选用一些数据进行小范围的循环圈长度、循环圈个数以及总循环长度 (阶) 测试，然后固定 N 进行随机的混沌因数和种子计算 N 的平均阶，绘制“平均阶-N”的曲线分析

2.3 选择混沌映射

本文选择了三种混沌映射：

Logistic 映射:

$$x_{n+1} = \mu x_n(1 - x_n) \quad (0 < x < 1)$$

在 $3.57 < \mu < 4$ 呈现混沌特性

Cubic 映射:

$$x_{n+1} = r x_n(1 - x_n^2) \quad (0 < x < 1)$$

在 $2.5 < r < 3$ 呈现混沌特性

Sine 映射:

$$x_{n+1} = \frac{4}{a}\sin(\pi x_n) \quad (-1 < x < 1)$$

在 $0 < a < 4$ 呈现混沌特性

3 系统测试与结果

3.1 测试方案

选择在 python 平台上进行代码编写，对于循环圈长度、循环圈个数和阶采用几组随机数据测评；对于“平均阶-N”采用生成随机的 x_0 和 μ，并生成数据，将数据写入 Excel 表格内，再利用 Origin 分析软件进行拟合的方式进行分析。

3.2 功能测试与分析

3.2.1 Logistic

由于 $3.57 < \mu < 4 \quad (0 < x < 1)$ 中呈现混沌特性，我选取以下几组数据 $[(x_0, \mu, N)]$(M 选择 1000) 进行测试：

(0.66,3.66,40)	(0.66,3.66,80)	(0.66,3.66,120)
循环数量 4	循环数量 6	循环数量 6
循环长度 [33,3,3,1]	循环长度 [27,19,27,3,2,2]	循环长度 [48,48,7,7,3,7]
阶 33	阶 1026	阶 336
循环 33 有 1 个	循环 27 有 2 个	循环 48 有 2 个
循环 3 有 2 个	循环 19 有 1 个	循环 7 有 3 个
循环 1 有 1 个	循环 3 有 1 个	循环 3 有 1 个
	循环 2 有 2 个	

可以看到，最大循环长度基本是随 N 递增而增大的，由于第三组中最大的循环长度相等，所以阶会比第二组小。对于 N 比较小的情况下，Logistic 混沌置乱下的小循环比较多，这个对于安全性是不是很有利。

以下是经过拟合的“平均阶-N”图像：

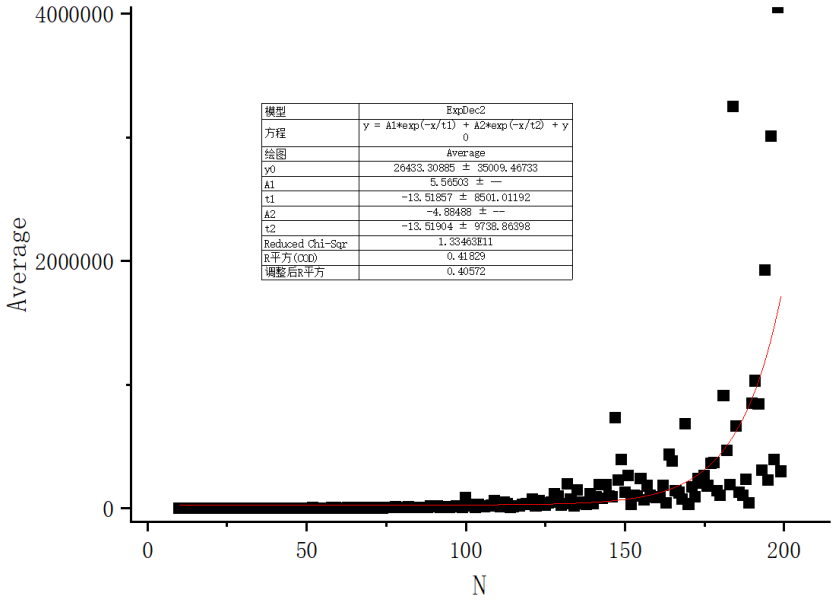

图 1: Logistic 映射置乱

可以看到，平均阶-N 图像基本是以指数增长的形式增长的，也就是说，N 越大，复原置乱所需要的置乱次数基本成指数级增长，在 N 为 200 左右的时候，平均阶的数量级在 $10^5 \sim 10^6$，在 N 足够大的是后表现良好

3.2.2 Cubic

Cubic 映射在 $2.5 < 3r \quad (0 < x < 1)$ 的时候呈现混沌特性，选取以下几组数据进行测试：

(0.68,2.83,40)	(0.68,2.83,80)	(0.68,2.83,120)
循环数量 2	循环数量 6	循环数量 6
循环长度 [37,3]	循环长度 [39,16,4,16,4,1]	循环长度 [61,27,27,2,2,1]
阶 111	阶 624	阶 3294
循环 37 有 1 个	循环 39 有 1 个	循环 61 有 1 个
循环 3 有 1 个	循环 16 有 2 个	循环 27 有 2 个
	循环 4 有 2 个	循环 2 有 2 个
	循环 1 有 1 个	循环 1 有 1 个

可以看出测试数据中阶关于 N 的增长比较大，性能相较于上面讨论的 Logistic 混沌置乱更强，以下是经过拟合的“平均阶-N”图像：

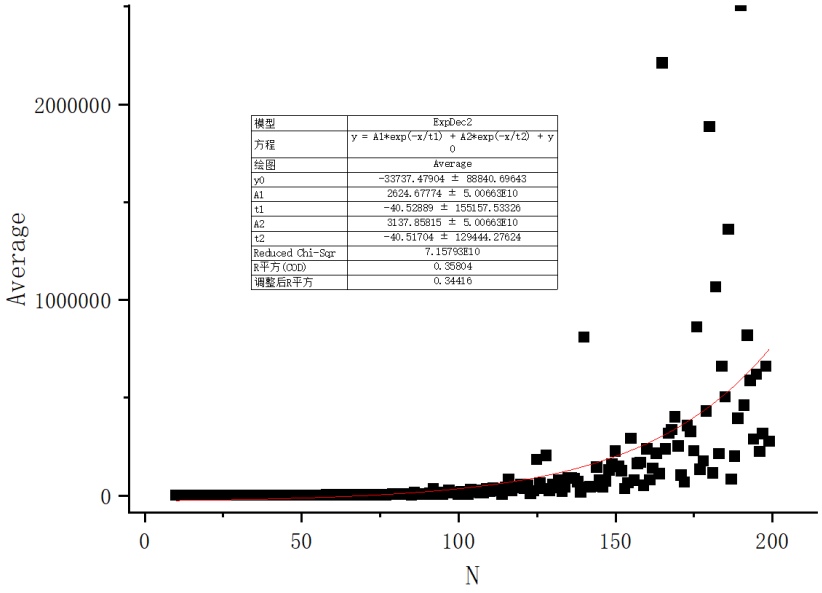

图 2: Cubic 映射置乱

从曲线整体的走势可以看出 Cubic 混沌置乱在 N 相对较小的情况下，可以带来相较于 Logistic 混沌置乱更强的安全性，复原一个序列需要的计算量更大。

3.2.3 Sine

(0.31,3.62,40)	(0.31,3.62,80)	(0.31,3.62,120)
循环数量 8	循环数量 4	循环数量 10
循环长度 [10,2,7,2,7,10,1,1]	循环长度 [25,33,11,11]	循环长度 [13,65,2,3,5,7,13,7,3,2]
阶 70	阶 825	阶 2730
循环 10 有 2 个	循环 25 有 1 个	循环 13 有 2 个
循环 2 有 2 个	循环 33 有 1 个	循环 65 有 1 个
循环 7 有 2 个	循环 11 有 2 个	循环 2 有 2 个
循环 1 有 2 个		循环 3 有 2 个
		循环 5 有 1 个
		循环 7 有 2 个

根据测试数据，Sine 映射的循环圈数量较多，影响局部安全性。

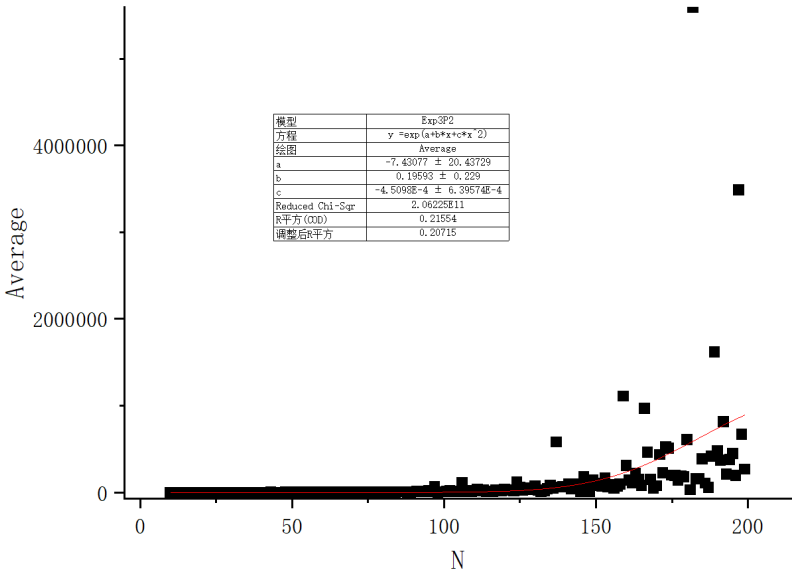

图 3: Sine 映射置乱

从图像可以看出 Sine 混沌置乱的平均阶增长较为缓慢，相较于前面两个混沌映射，安全性更弱

4 应用前景

混沌置乱可以应用在图像的加密，加密效果如下图所示：

原图、Logistic 加密、解密后的图像：

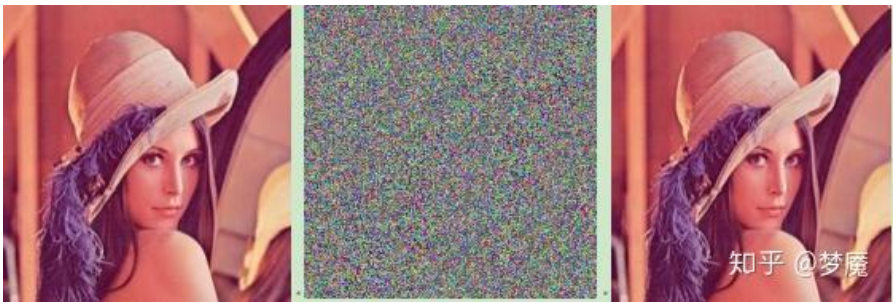

图 4: Lena 图

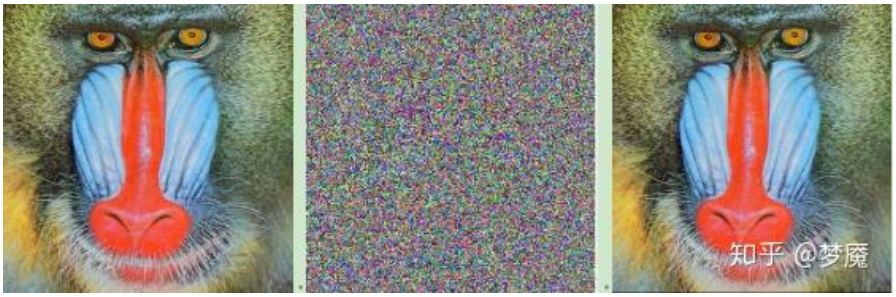

图 5: Baboom 图

图片来源：[1]

由于计算复杂度低，混沌置乱适合实时加密，还可以用于视频流加密、通信安全等领域。

5 结论

本文对三个不同的混沌置乱进行了简短的分析，总结得出三个置乱中 Cubic 混沌置乱的效果最好，而且置乱的安全性基本随着 N 的增大呈指数级增长，N 足够大时可以获得较强的安全性。

参考文献

[1] 知乎用户. 基于混沌 Logistic 加密算法的图片加密与还原 [EB/OL]. 知乎专栏, 2021.https://zhuanlan.zhihu.com/p/183788811