混沌图像加密算法设计与性能分析

華東交通大學
EAST CHINA JIAOTONG UNIVERSITY

目录
content

研究背景

2013年6月6日，前中情局（CIA）职员斯诺登先后通过英国《卫报》和美国《华盛顿邮报》曝光了美国国家安全局（NSA）的一项绝密电子监听计划——**棱镜计划（PRISM）**

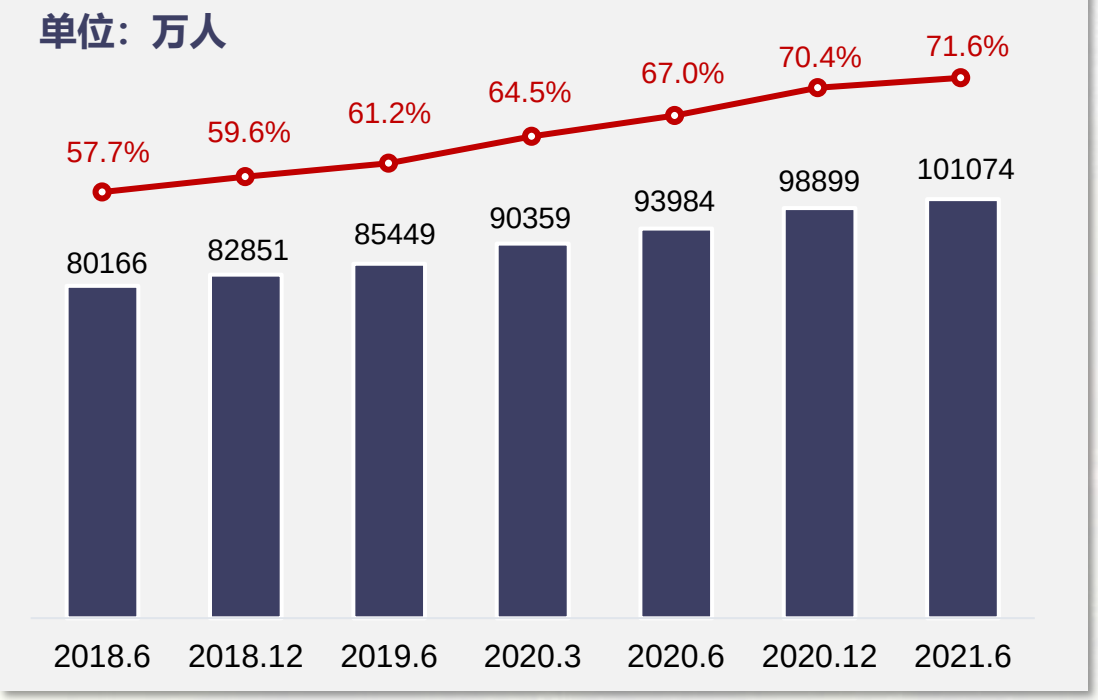
该计划自2007年起开始实施，监视范围很广，**电邮、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间**和**社交网络资料的细节**都在监控之列。通过该项目，美国国家安全局甚至可以实时监控一个人正在进行的网络搜索内容。

研究背景

随着5G的普及，

图像视频信息占了网络信息的 **70%**

网民规模和互联网普及率



来源：CNNIC 中国互联网发展状况统计调查

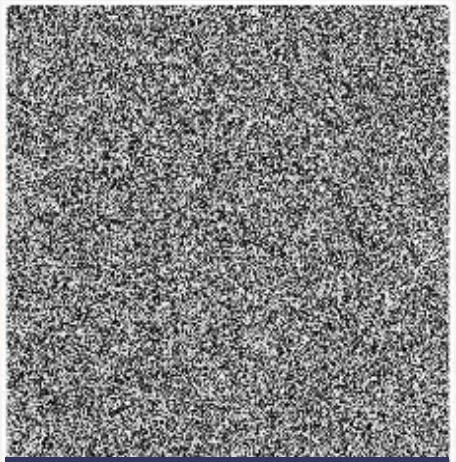
数字图像是一种特殊的信息表达载体形式

保护图像中的隐私信息**十分重要**

用于保护数字图像隐私安全的传统方法

图像水印

主要是指在明文图像中嵌入数字水印，以保护相关明文图像的版权。



图像加密

主要是通过可逆数学变换对图像的像素进行操作，使得变换前后的数字图像尽量不相关

研究背景

混沌系统

- 初值敏感性
- 不可预测性
- 伪随机性

被广泛地应用在图像信息安全领域中

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

性能对比

1-D

1-D 混沌映射

1-D 混沌映射进行图像加密时，有几种加密算法被认为是不安全的

H-D

H-D 混沌映射

H-D 混沌映射具有更复杂的结构和更好的混沌性能然而，它们的硬件实现相对复杂和昂贵，并且计算的速度较慢。

设计任务

01

了解混沌及其加密设计基本原理

02

分析掌握已有混沌图像加密方法

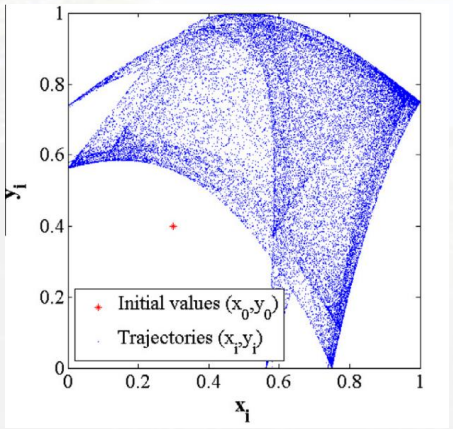
03

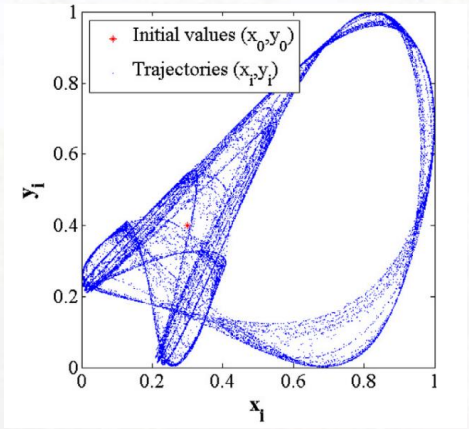
设计可行的混沌图像加密算法

04

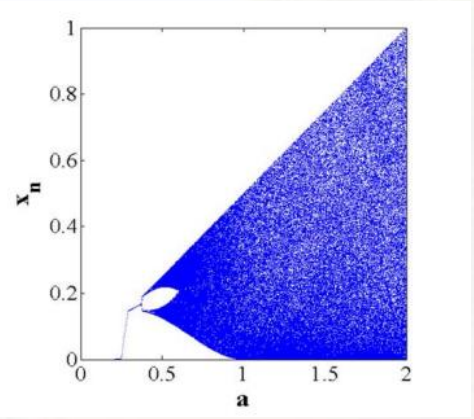
分析混沌图像加密算法的具体性能

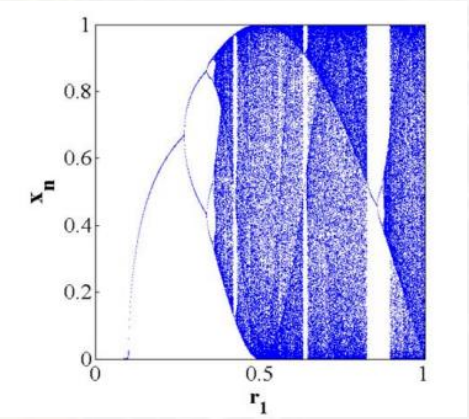
典型系统



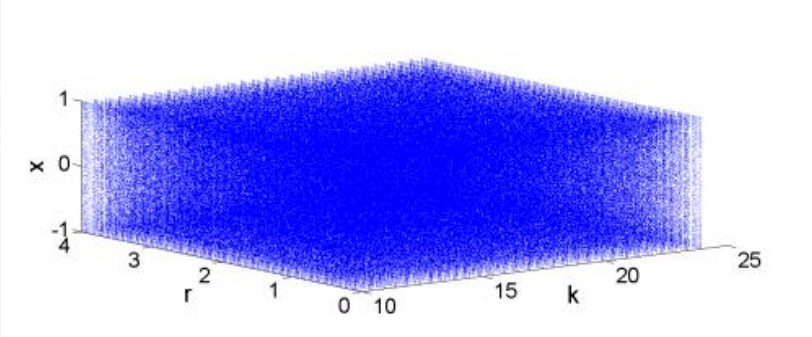


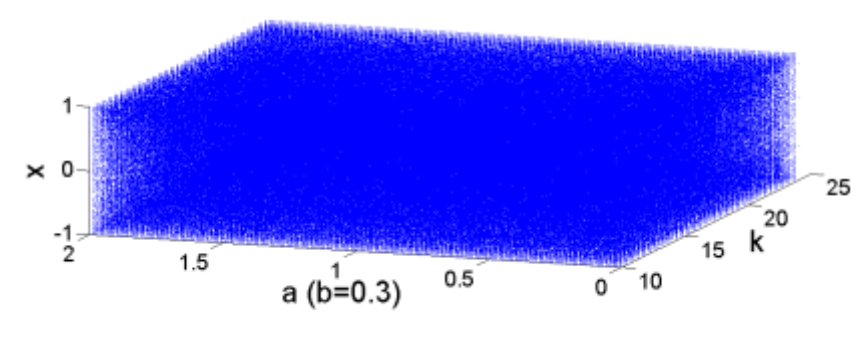
文献[48]中提出的2D-SLMM混沌系统





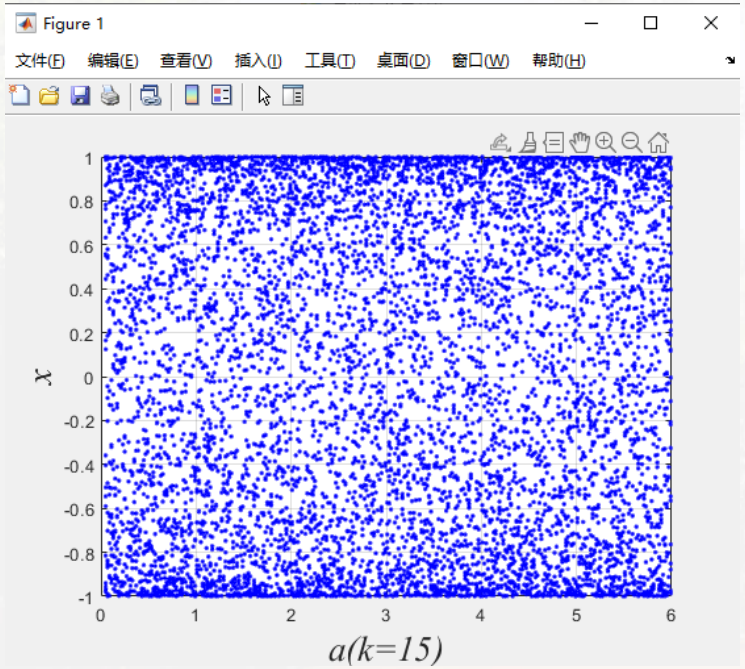
文献[44]中提出的logistic-tent、double-sine混沌系统

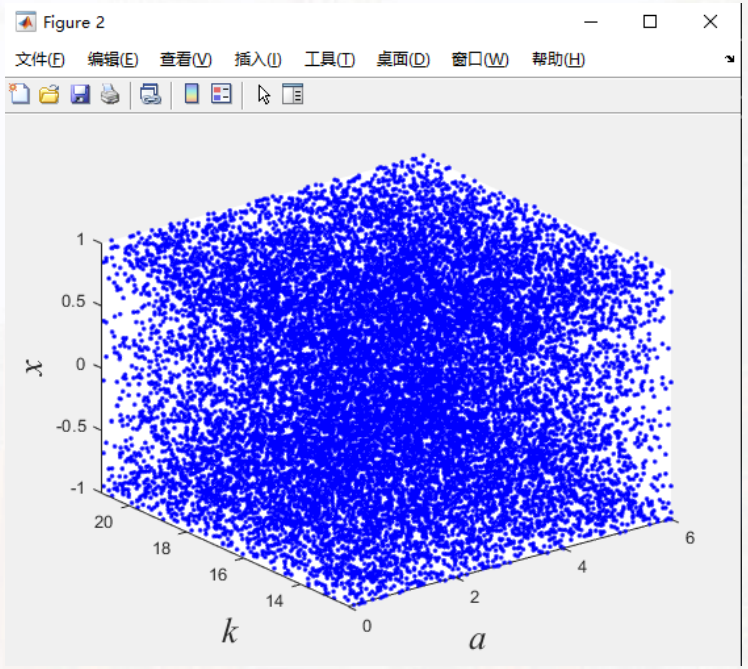




文献[45]中提出的CLM、CHM混沌系统

ISCM混沌系统





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

本设计提出了一种1-D和2-D级联的混沌系统，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**方面都较好。

混沌奇异变换CMT

混沌矩阵 ***S***　　排序后矩阵 ***R***　　索引矩阵 ***I***

以索引矩阵第一行为例

明文图像 ***P***　　打乱后的像素矩阵 T_1

输入：原始图像矩阵P和混沌矩阵S（大小均为M × N）

1：使用sort函数对S的各列进行大小排序，得到排序结果

2：生成排序矩阵I：

3：for *i* =1:M do

4：将图像矩阵P的像素 连接成一个圆形队列

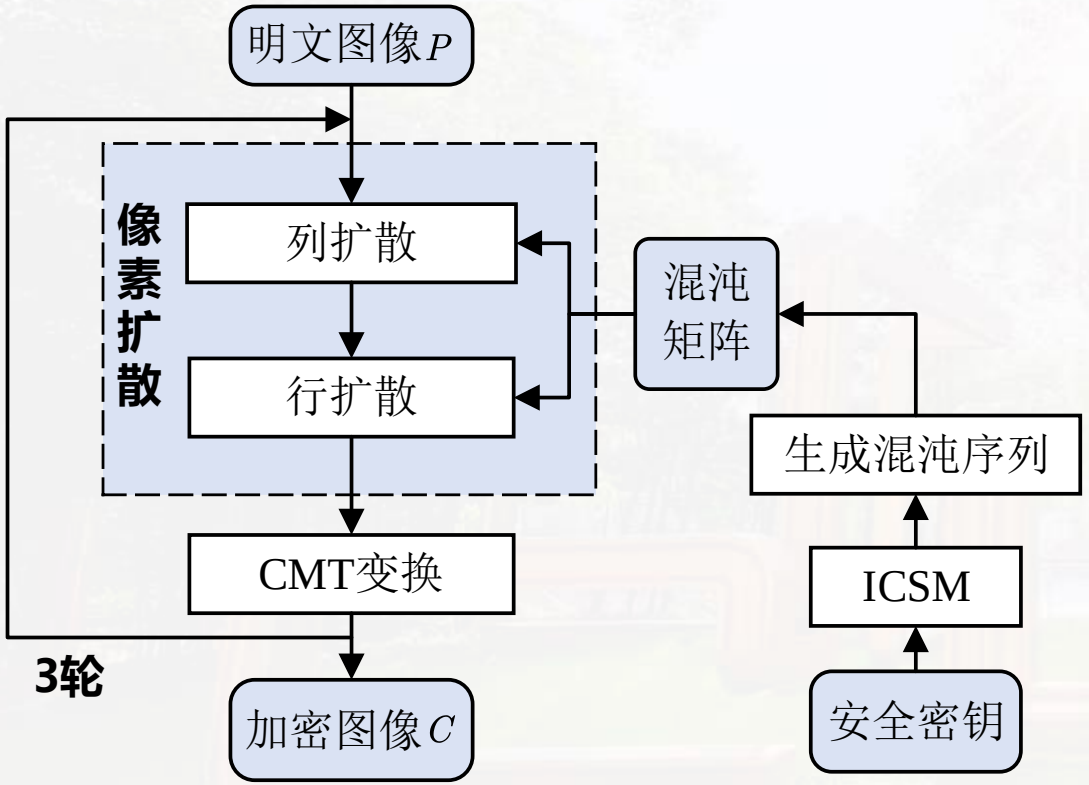
5：对这些关联起来的像素串进行向右平移 个单位

6：end for

输出：加密图像 T

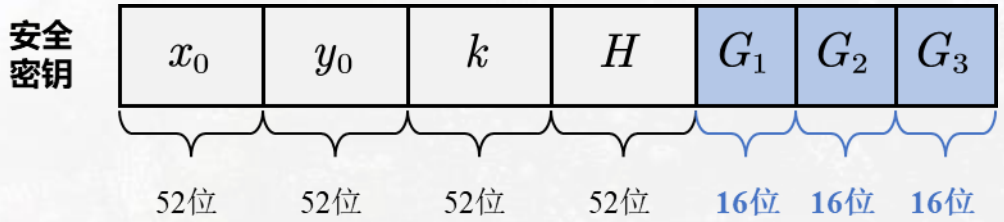
CMT-ICSM加密算法

加密算法流程图



解密算法即为加密算法的逆过程

(1) 生成初始条件



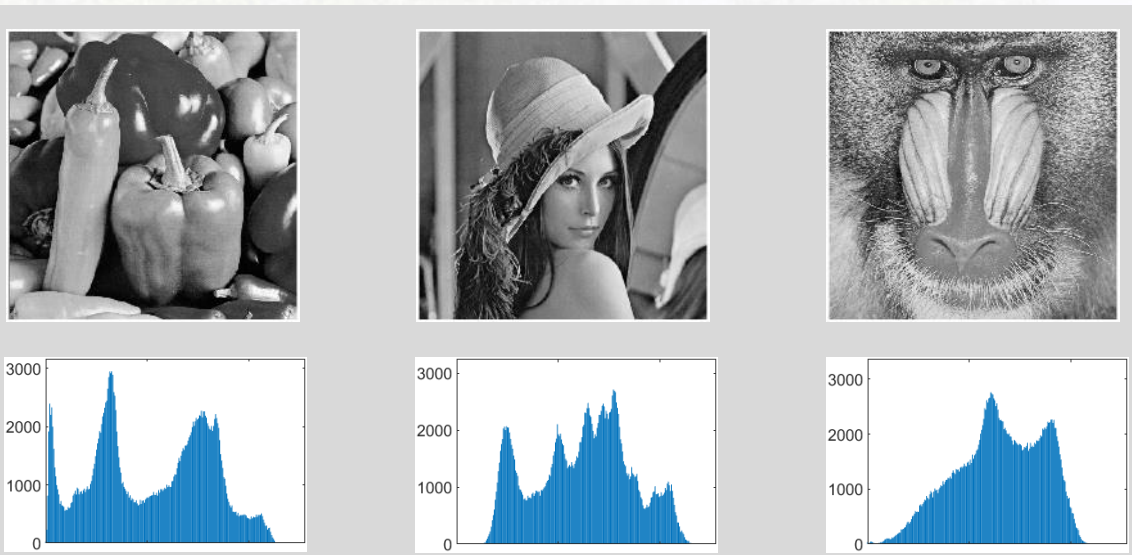
使用随机生成二进制数的方法来生成密钥

(2) 图像加密

经过3轮CMT变换和扩散，生成加密图像

性能分析

CMT-ICSM



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

仿真结果表明，本设计提出的CMT-ICSM算法能够将不同的图像转换为**像素值随机均匀分布的类噪声加密图像**，具有良好的加密性能。

性能分析

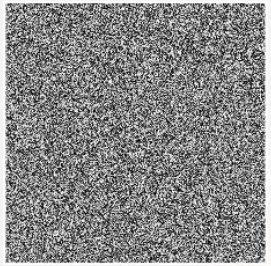
密钥敏感性

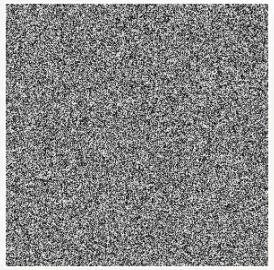
加解密过程中，密钥出现任何变化都会令结果不一样

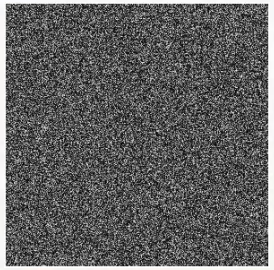
假设K1，K2，K3为三个仅相差一位的密钥

加密过程

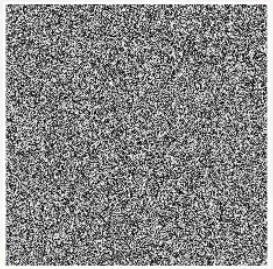

原图


K1加密

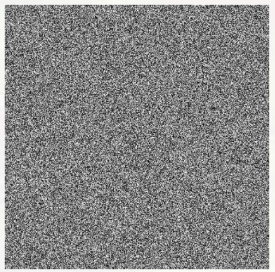

K2加密


K1-K2

解密过程


K1加密


K1解密


K3解密

差分攻击分析

两图的变化像素数(NPCR)和平均变化强度数(UACI)

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

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

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

与理想值99.6094%和33.4635%非常接近，能较好抵御差分攻击

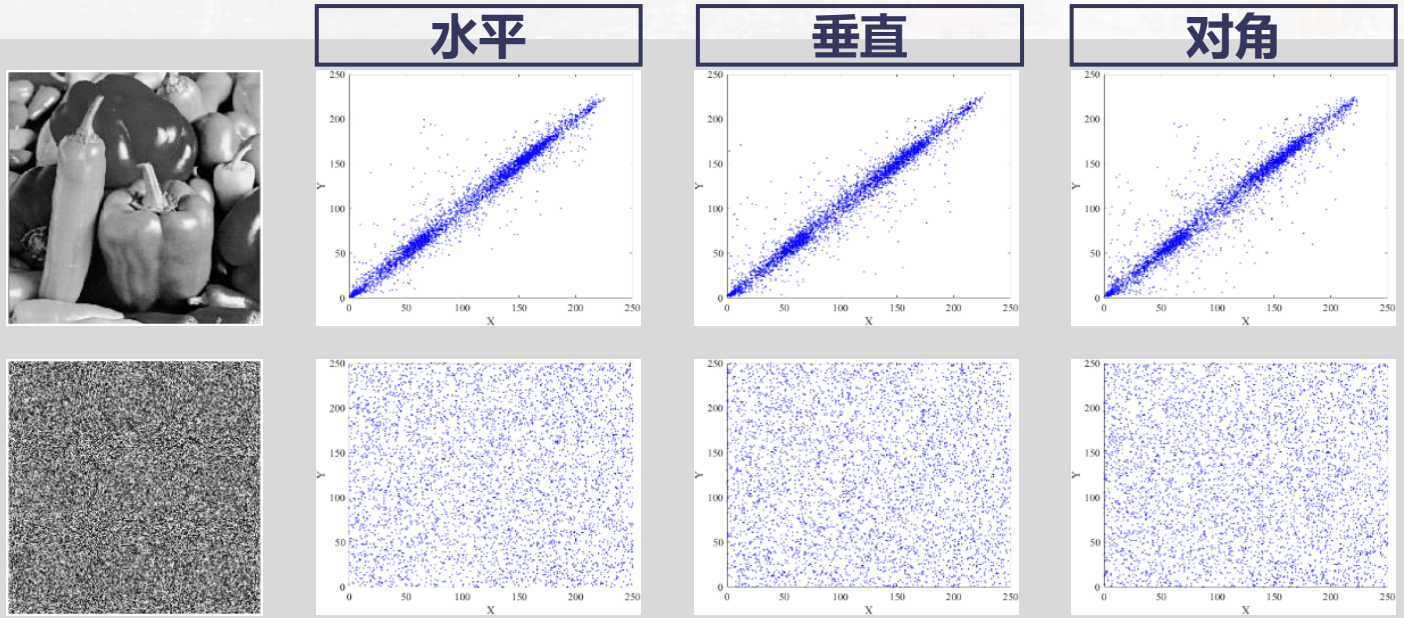
性能分析

相邻像素相关性分析

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

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

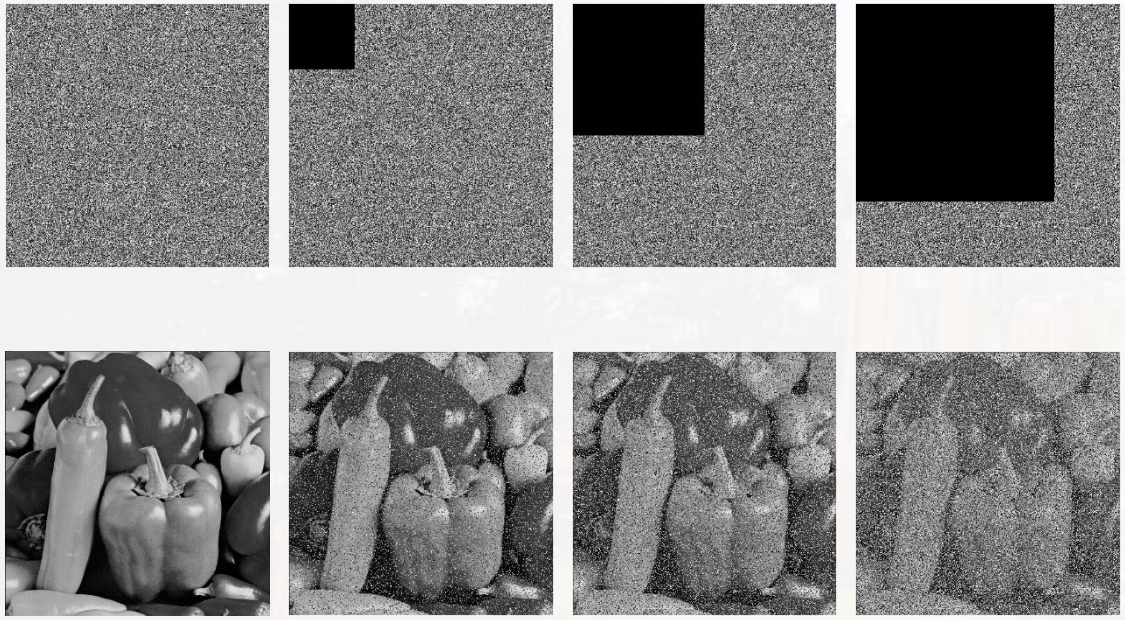
图像	水平	垂直	对角
原始图像	0.982856	0.979426	0.968485
加密图像	0.003554	0.006477	-0.001736



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，可以看出，加密后的图像邻近像素基本上**不具有相关性**

性能分析

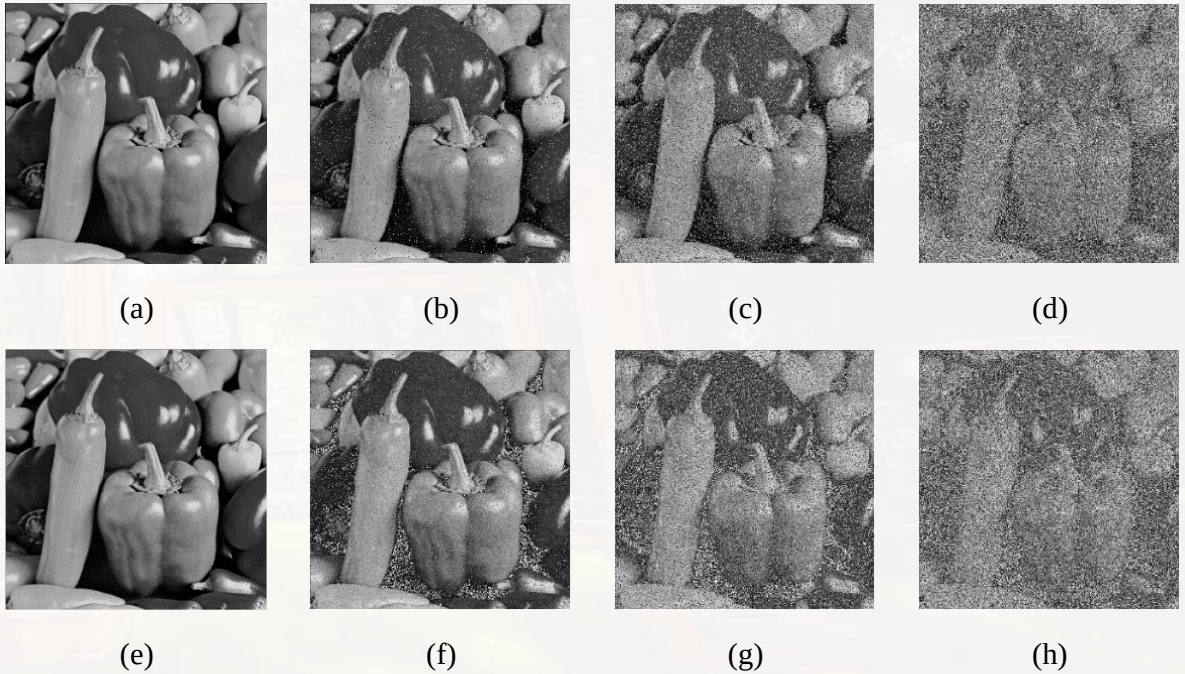
抗裁剪攻击分析



抗噪声攻击分析

(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

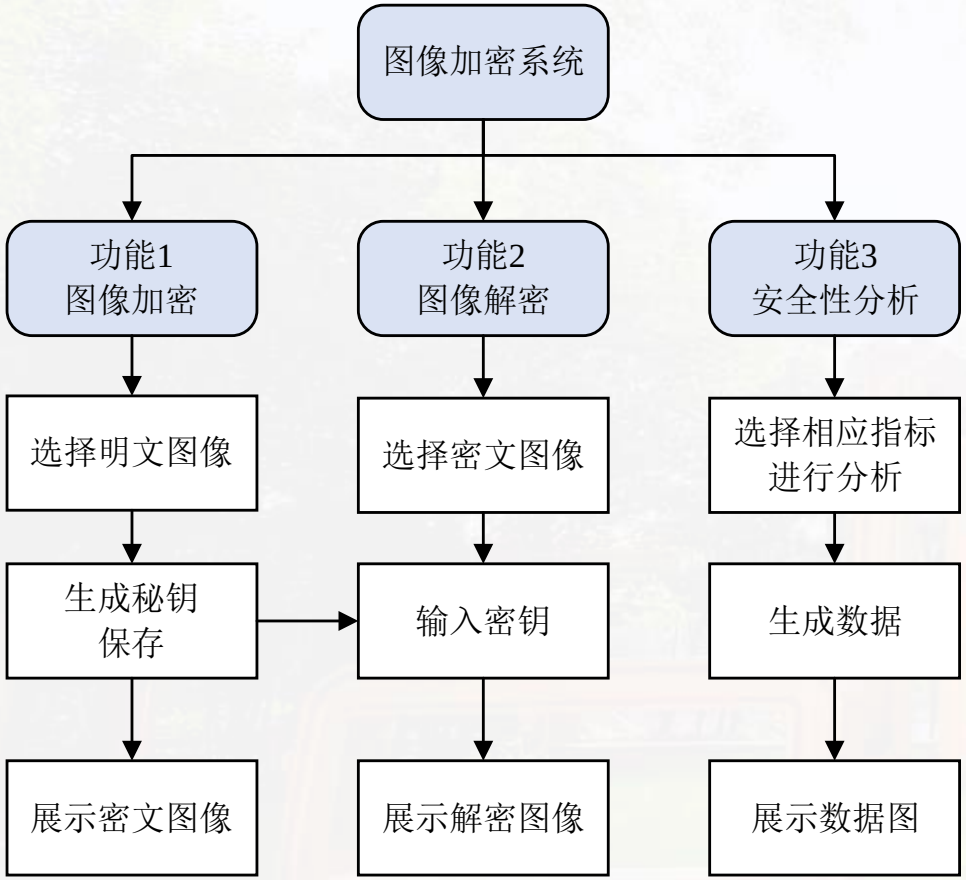


(a) (b) (c) (d)

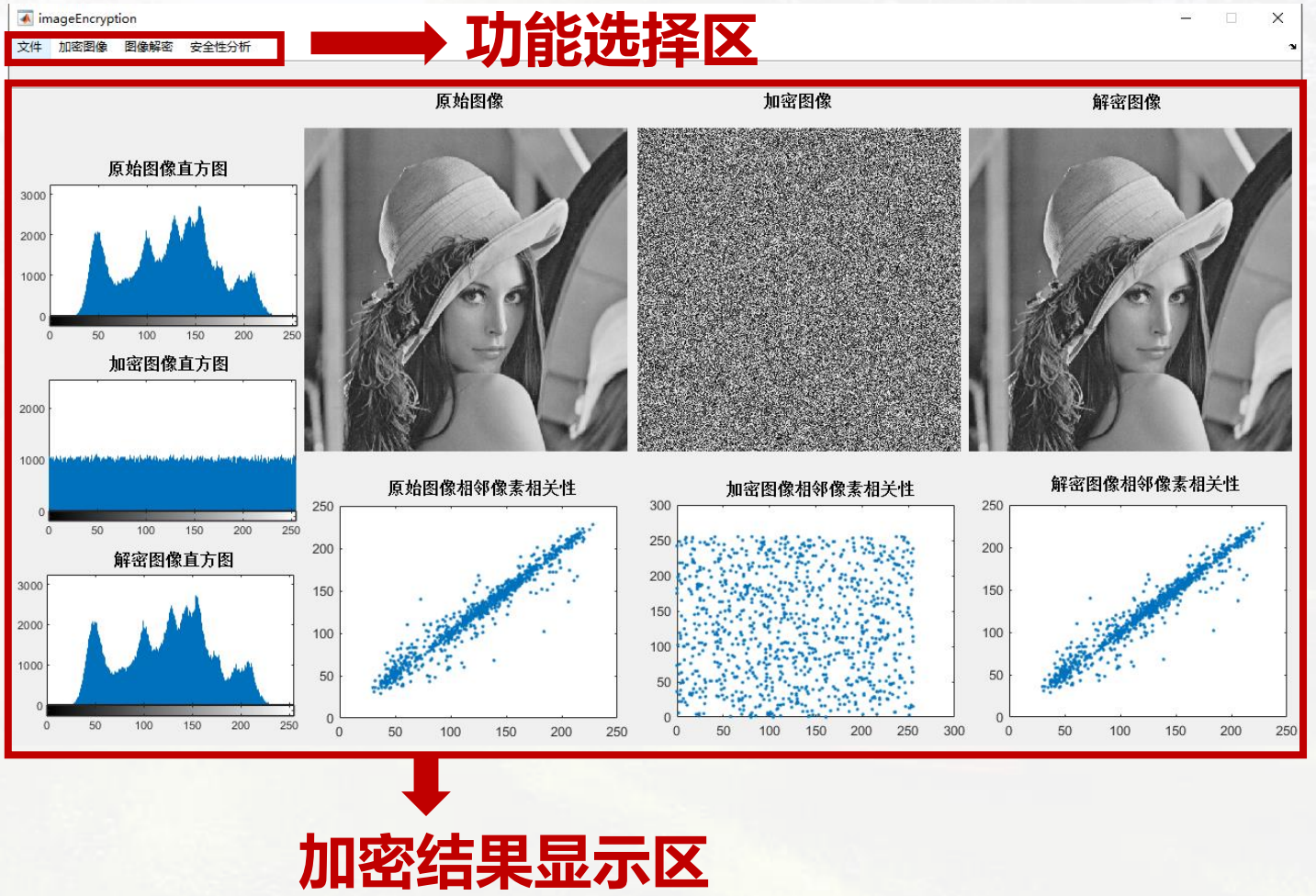
(e) (f) (g) (h)

当加密图像遭到破坏或噪声时，经过本算法解密出的图像仍然具有很好的可读性

图像加密系统GUI设计



加密系统功能图



图像加密系统GUI设计

混沌图像加密系统GUI演示

创新点与展望

创新点

01

提出一种新的级联系统

ICSM具有混沌范围更宽广、更好的遍历性和混沌性能等优势

02

设计一种新的加密算法

结合ICSM和CMT，创新地设计了算法结构，提出了一种新的图像加密算法(CMT- ICSM)

03

设计了一款图像加密GUI

能供科研人员测试与开发，提升进行科学研究的效率

展望

加密算法仍存在一定规律，未来可尝试采用机器学习、神经网络等方法自适应调整混沌系统参数

请老师们批评指正

East China Jiaotong University