

**CSE 309 第一次作业**

**面向图像的秘密共享**

2023年11月08日

**学院：网络空间安全学院**

**专业：网络空间安全**

**学生姓名： 姚俨璁 学 号：21312719**

## 一、算法原理简介

基于Shamir秘密共享协议的图像秘密共享方案：

一、基本原理与思想

Shamir秘密共享协议：假设一个秘密s，秘密分发者将s运用特定算法分成n份，然后将n份分别分发给n个参与者。在重构时，n个参与者中选取r个人来重构这个秘密。任意的r个人都可以重构，任意的r-1个参与者无法获得秘密的任何信息。

二、将上述基本思想应用到图像领域

2.1 灰度图像处理思路

灰度图像是由一系列像素值组成，可以把每个像素值都视作一个秘密s，利用shamir秘密共享协议的基本原理，用随机生成的多项式生成n份子秘密，遍历所有的像素点即可生成相应的n份影子图像。在重构阶段，随机选取任意r份影子图像，对各个像素点应用拉格朗日插值公式以恢复原像素点，遍历所有的像素点即可恢复原秘密图像。

2.2 具体算法

分发阶段：

1. 读取图像，将图像转换成数组形式，并展平成一维数组，方便后续操作。

2. 对像素值进行预处理：由于shamir秘密共享方案中的多项式需要选取一个素数p，而像素值范围为0~255，因此我们选择小于255的最大素数251作为素数p（选取的素数应小于255，若大于255则会出现秘密值大于255的情况，无法以图像形式分发或无法完全恢复图像）。为保证分发和恢复过程中的损失尽量小，我们提前将读取的图像中像素值大于250的像素值都修改为250。

3. 使用一个exceed列表存储那些超过250的像素值与250的差值，作为后续无损恢复的凭证。该凭证可依附于分发图像进行分发，也可以交付给可信第三方进行保管。

4. 严格按照shamir秘密共享算法，随机在p的有限域内生成多项式系数，接着根据r的值确定多项式的次数，计算得出n个秘密影子图像的像素值。

5. 将生成的影子图像一维数组reshape成原本形状并进行保存分发。

恢复阶段：

1. 为了方便测试，我读取所有分发的影子图像，并且随机选取r个影子图像的像素值数据用作恢复图像。

2. 重点：利用拉格朗日插值公式恢复秘密。由于我们的多项式取251的模，如果多项式中的系数或常数项（秘密值）出现分数，则需要计算分母的逆元（模251条件下），并同时乘分母与其逆元（在模251条件下相当于乘1），将分数化为整数值。

3. 重点：执行完上述步骤后，遍历生成的恢复后的一维数组，若恢复的秘密值等于250，则查询在分发阶段生成的exceed列表，利用该列表的内容恢复其原本的像素值，实现无损恢复。

验证、评估阶段：

逐像素对比原图与恢复图像的像素值，若有不一致的像素值，则输出该像素的位置，并输出原来的像素以及恢复后的像素。若没有不一致的像素值，则输出“两个图像的像素完全一致”。

## 二、新的探索 【加分项】

上述思路针对的是灰度图像，但其实RGB图像也同理。RGB图像有三个通道，在分发阶段我们可以分别将三个通道视作灰度图像进行处理，再进行分发；恢复阶段可以将三个通道的图像叠加以恢复RGB图像。

或者直接将RGB图像展平（flatten），逐个像素值进行处理，最后在reshape成原来的形式。其余步骤同上述步骤。

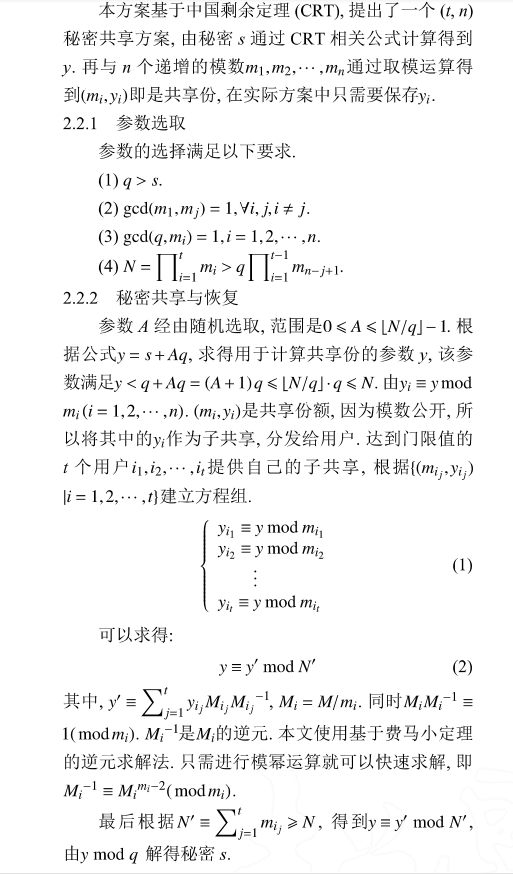
综上，彩色图像和灰度图像在本算法中处理方式是相同的。

由于shamir秘密共享方案中的多项式需要模素数，在这个过程中可能会产生图像精度损失。本次实验采用exceed列表在读取图像时提前存储超过250像素的像素值与250的差值，以在恢复阶段恢复原本的像素值，实现无损。

基于中国剩余定理（CRT）的图像秘密共享算法（未实现，只是讲一下算法思路）  
参考文献：

陈维启,张珍珍,李祯祯,丁海洋,李子臣.基于 C RT 的无损高效门限彩色图像秘密共享信息隐藏算法.计算机系统应

用,2022,31(5):269-276. <http://www.c-s-a.org.cn/1003-3254/8429.html>



由于CRT秘密共享算法在彩色图像应用实现上会出现像素溢出问题，将超过255像素值的共享数据根据上文分别存成倍数图像与余数图像。

标黄的思路也可以应用于我本次实现的基于shamir秘密共享的图像共享方案。也可以实现无损。

## 三、实验结果分析

3.1 实验结果截图简要分析。

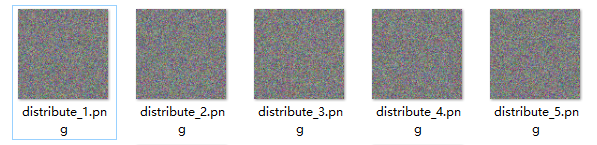
3.2 新的探索算法结果分析。

两个合二为一进行分析（最终实现的效果）：

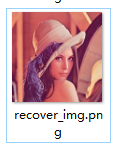
原始图像：



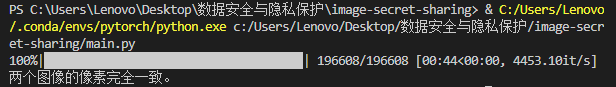
分发的五个影子图像：



恢复图像：

终端运行的结果：



验证部分的输出为“两个图像的像素完全一致”，可以看到完全恢复了原有的图像。

测试的图像为256×256×3，故总共要处理的像素值为196608。

整个项目的文件夹：

