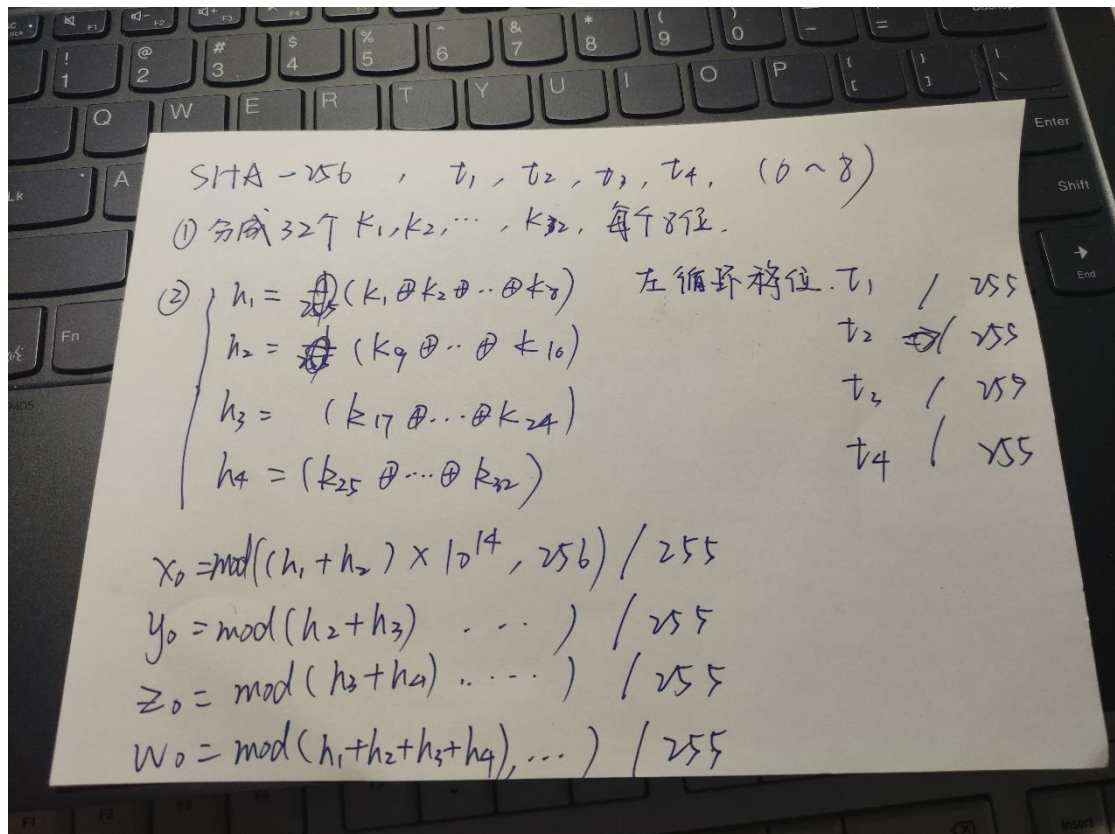


# 1 密钥


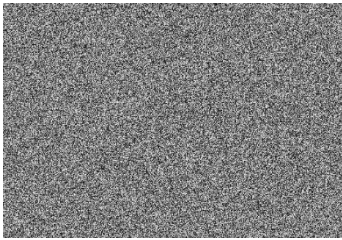

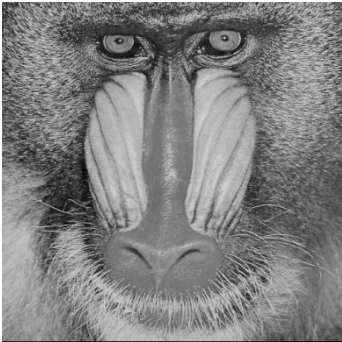
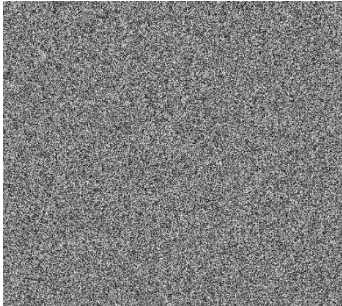


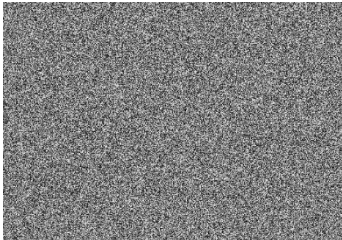
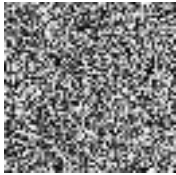

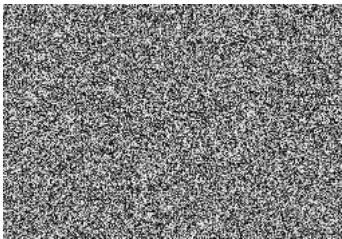

三部分组成,

1. 待加密图像的 sha-256 的哈希值 ( $2^{256}$ )
2. 循环移位值  $t$  ( $10^4$ )




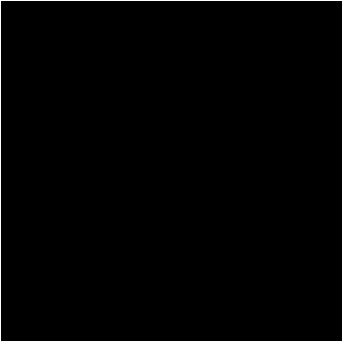




## 2 加密结果

### 2.1 图像测试结果

图片编号	原始图像	加密图像	缩略图加密图像
Lena			
Mandrill			
Peppers			
Camera			

---

White			
Black			

## 2.2 信息熵

图片编号	原始信息熵	加密后信息熵	缩略图信息熵
Lena	7.4456	7.9989	7.9534
Mandrill	7.3579	7.9993	7.9550
Peppers	7.5715	7.9989	7.9531
Camera	7.0097	7.9962	7.7803
White	0	7.9976	7.9578
Black	0	7.9972	7.9553

## 2.3 密钥敏感性

Lena 加密密钥:

Key1:


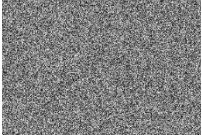


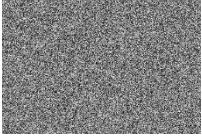



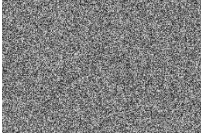

25722568D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0  
FFA599AE6A9





Key2:

15722568D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0  
FFA599AE6A9

Key3:

25722568D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0  
FFA590AE6A9

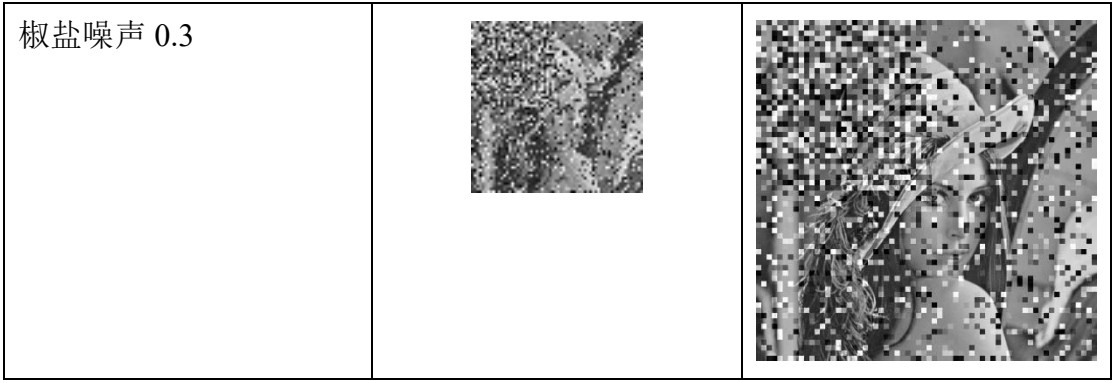
	缩略图加密图 像	缩 略 图 和 Key1 的差	完整加密图像	完 整 图 像 和 Key1 的差
Key1		就是自身		就是自身
Key2				
Key3				

	缩略图	完整图像
用 Key1 解密 Key1 加密图像		
用 Key2 解密 Key1 加密图像		因为破坏了 DC 编码的前缀码的规则，无法解码，就没有完整解密图像
用 Key3 解密 Key1 加密图像		因为破坏了 DC 编码的前缀码的规则，无法解码，就没有完整解密图像

## 2.4 抗噪声

噪声加在缩略图上，如果加在完整图像上，还是由于 DC 编码部分无法解码，导致没有解密的完整图像。

	缩略图	完整图像
椒盐噪声 0.1		



## 2.5 相关性

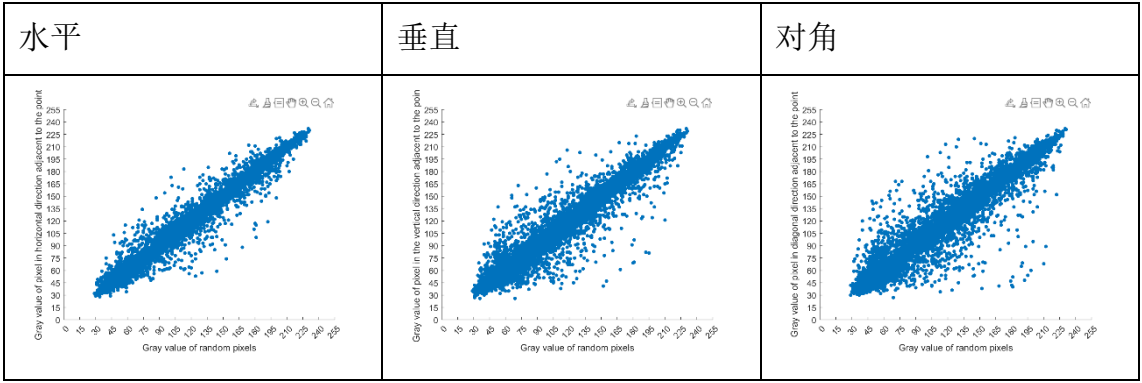
Lena

原始图像

水平相关性=0.96991

垂直相关性=0.98514

对角线相关性=0.95701

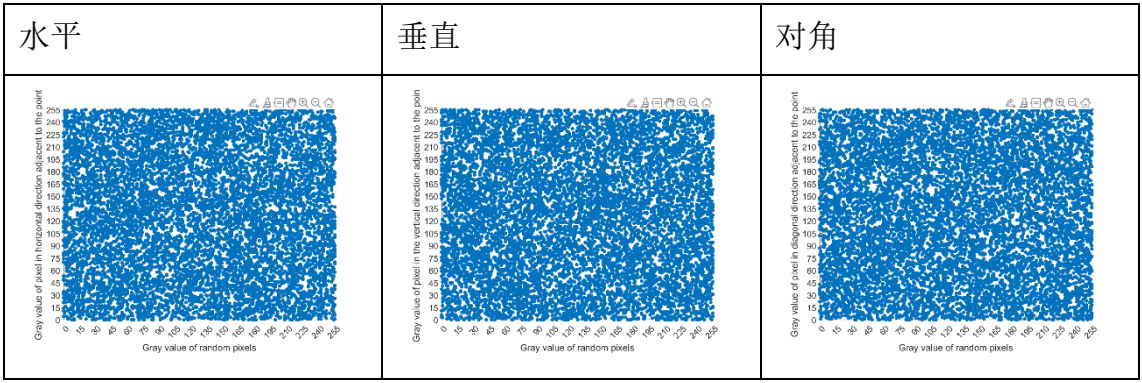


加密图像

水平相关性=-0.008348

垂直相关性=-8.7074e-05

对角线相关性=0.006379



---

## 2.6 时间

加密一张  $512 \times 512$  的灰度图并存储加密数据大概在 5s 左右，大部分时间花在 DC 编码和储存加密数据时的二进制转换上面。