# 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）

文本, 信件

描述已自动生成

# 加密结果

## 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 | 女人戴着帽子  描述已自动生成 | 在地毯上  中度可信度描述已自动生成 | 地毯上的刺猬  描述已自动生成 |
| Mandrill | 猴子的脸  描述已自动生成 | 在地毯上  中度可信度描述已自动生成 | 地毯上的刺猬  描述已自动生成 |
| Peppers | 桌子上有许多水果  中度可信度描述已自动生成 | 在地毯上  中度可信度描述已自动生成 | 地毯上的刺猬  描述已自动生成 |
| Camera | 图片包含 户外, 人, 物体, 水  描述已自动生成 | 在地毯上  中度可信度描述已自动生成 |  |
| White | 图片包含 形状  描述已自动生成 | 黑白色的照片  中度可信度描述已自动生成 | 地毯上的刺猬  描述已自动生成 |
| Black | 形状  低可信度描述已自动生成 | 草地上有地毯  描述已自动生成 | 在地毯上  描述已自动生成 |

## 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 |

## 密钥敏感性

Lena加密密钥：

Key1:

**25722568D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0FFA599AE6A9**

Key2:

**15722568D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0FFA599AE6A9**

Key3:

**25722568D126918052AB7B93683092B4043A5C2BB3110BC260627601EAE0FFA590AE6A9**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 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 |  | 因为破环了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 |  | 因为破环了DC编码的前缀码的规则，无法解码，就没有完整解密图像 |

## 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 |  |  |
| 椒盐噪声0.3 |  |  |

## 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

|  |  |  |
| --- | --- | --- |
| 水平 | 垂直 | 对角 |
|  |  |  |

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

|  |  |  |
| --- | --- | --- |
| 水平 | 垂直 | 对角 |
|  |  |  |

## 时间

加密一张512\*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。