

## 实验二 专用隐写分析（一）

姓名：王运韬

学号：201628018627123

### 一、实验目的：

理解卡方分析<sup>[1]</sup>的原理，采用其攻击 *JSTEG* 算法<sup>[2]</sup>，并验证 *OUTGUESS* 算法<sup>[3]</sup>的改进。

### 二、实验原理：

*LSB* 类型的隐写算法会改变媒体数据的直方图对值分布特征，具体来说，媒体数据直方图中取值为  $(2i, 2i+1)$  的对值分布频数在嵌入秘密信息后将趋于接近。

卡方分析的基本原理是，利用媒体数据直方图的  $r$  统计量衡量这种媒体数据直方图对值分布的变化，以此作为判断媒体数据中是否含有秘密信息的依据。 $r$  统计量定义为：

$$r = \sum_i \frac{(n_{2i} - n_{2i}^*)}{n_{2i}^*}$$

它符合卡方分布，其中， $n_i$  表示媒体数据中取值为  $i$  的样点个数， $n_{2i}^*$  表示  $n_{2i}$  和  $n_{2i+1}$  的均值。

当对媒体数据按照 *LSB* 方式嵌入秘密消息后， $n_{2i}$  和  $n_{2i+1}$  的取值将趋于接近， $r$  统计量将减小， $r$  越小，表示媒体数据含有秘密消息的可能性越大。再结合卡方分布的密度函数即可计算隐写的可能性：

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}} \Gamma(\frac{k-1}{2})} \int_0^r \exp(-\frac{t}{2}) t^{\frac{k-1}{2}-1} dt$$

其中， $k$  表示媒体数据直方图对值得数量。如果  $p$  接近于1，则说明媒体中含有秘密消息。

### 三、实验步骤:

- 1.进行分析参数配置: 设置卡方分析的量化  $DCT$  系数检测区间;
- 2.攻击  $JSTEG$  算法: 对于  $JSTEG$  算法产生的载体和隐写样本, 计算它们的卡方分析值, 验证卡方分析检测  $LSB$  类型隐写算法的有效性;
- 3.攻击  $OUTGUESS$  算法: 对于  $OUTGUESS$  算法产生的载体和隐写样本, 计算它们的卡方分析值, 验证  $OUTGUESS$  在安全性上的改进。

### 四、实验结果:

#### 1.分析参数设置:

分别设定不同的检测区间, 求出其相应的  $p$  值, 计算隐写图像集和原始图像集的  $p$  均值, 找出差异较大的区间作为合适的  $DCT$  系数检测区间。

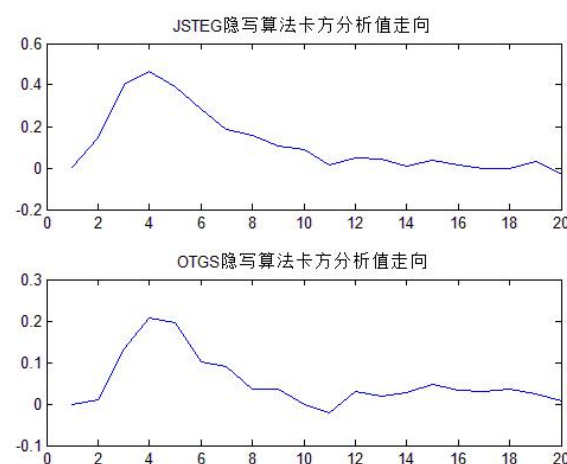


Fig 1. JSTEG 算法和 OTGS 算法卡方分析值走向图

根据实验可确定  $DCT$  系数检测窗口为:  $[4,5]$ , 即  $WinDown = 4$ ,  $WinUp = 5$ 。

在当前检测窗口下,  $JSTEG$  算法和  $OTGS$  算法产生的载体和隐写样本, 其卡方分析值分布直方图和散点图如下图所示:

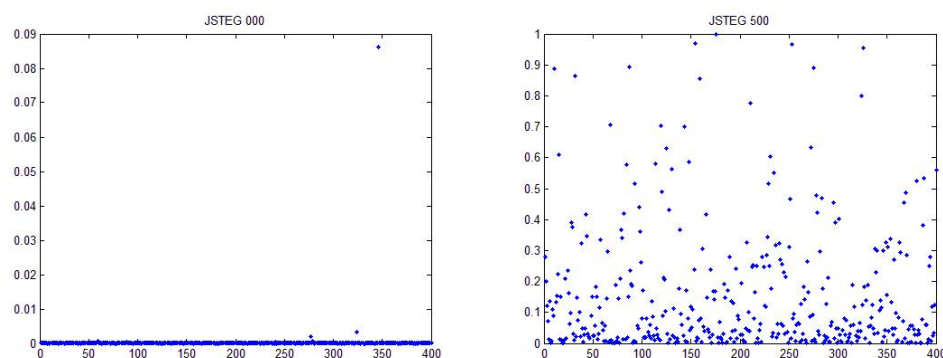


Fig 2. JSTEG 000 和 JSTEG 500 图像集卡方分析值散点图

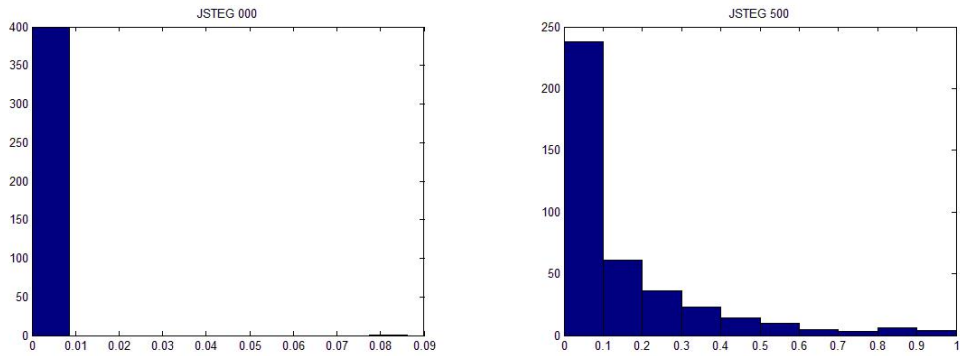


Fig 3. JSTEG 000 和 JSTEG 500 图像集卡方分析值分布直方图

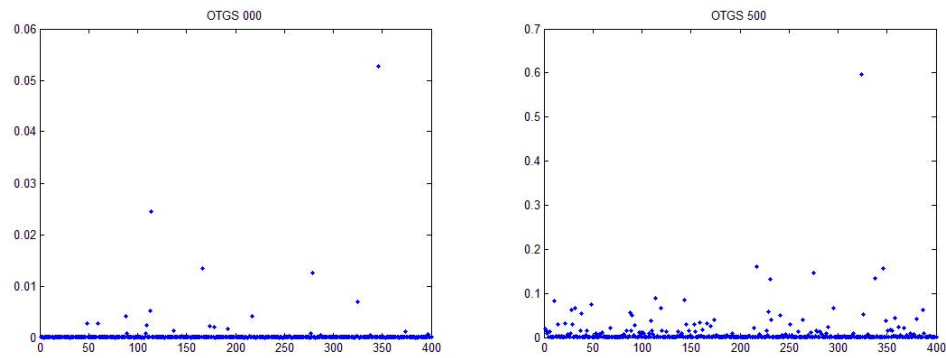


Fig 4. OTGS 000 和 OTGS 500 图像集卡方分析值散点图

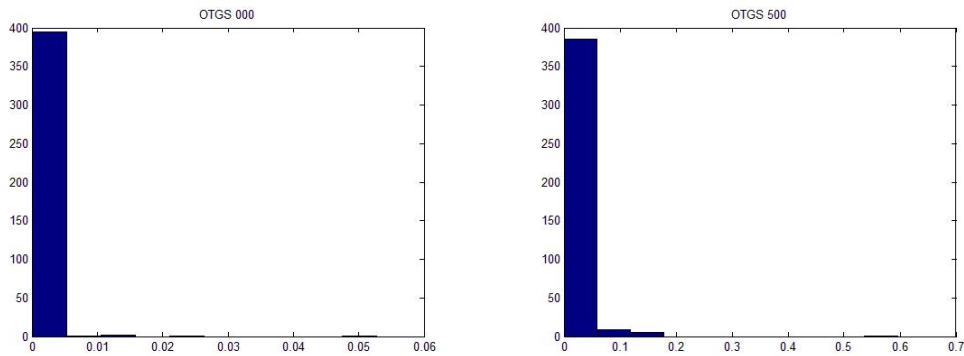


Fig 5. OTGS 000 和 OTGS 500 图像集卡方分析值分布直方图

取阈值  $T = 0.001$ ，对 *JSTEG* 算法进行隐写分析，虚警率  $FP = 0.0075$ ，真阳性率  $TP = 0.9775$ ，由此可得准确率为  $acc = 0.985$ 。可见，对 *JSTEG* 算法进行卡方分析可以有效进行判断载体是否发生隐写。

取阈值  $T = 0.0001$ ，对 *OTGS* 算法进行隐写分析，虚警率  $FP = 0.075$ ，准确率  $TP = 0.7725$ ，由此可得准确率为  $acc = 0.84875$ 。可见，对 *OTGS* 算法进行卡方分析可以有效进行判断其是否发生隐写。

从散点图也可知，*OTGS* 算法相对于 *JSTEG* 算法在安全性上有了较大的改进，可以较为鲁棒地抵抗卡方分析检测。

*analysis.m* 脚本为核心代码，用于对 *JSTEG* 算法和 *OTGS* 算法的卡方分析；

*analysis\_chisquare.m* 脚本用于分析参数配置，以选取合适的分析参数；

*figure\_chisquare.m* 脚本用于绘制对 *JSTEG* 算法和 *OTGS* 算法卡方分析所得分析值的散点图和分布直方图；

*accuracy\_chisquare.m* 脚本对图像集进行分析，以获得卡方分析对 *JSTEG* 算法和 *OTGS* 算法的隐写分析准确率。

## 五、实验结论

通过实验结果可知，卡方分析可以有效实现对 *JSTEG* 算法的隐写检测，从阈值设定和准确率可知，*OTGS* 隐写算法的安全性得到了较大提升。

总体来看，卡方隐写分析方法在针对连续 *LSBR* 的检测中准确率还是非常高的。

## 参考文献

- [1].Westfield, A. and Pfitzmann A., “Attacks on Steganographic Systems“, Proc. 3rd Info. Hiding Workshop, Dresden, Germany, September 28-October 1, 1999, pp. 61-75.
- [2].Jsteg, <ftp://ftp.funet.fi/pub/crypt/steganography/>
- [3].N. Proves. Defending against statistical steganalysis. The 10th USENIX Security Symposium, Washington, DC, USA, August 2001, pp.323-335.