基于LSB的隐写与隐写分析

雷敏

北京邮电大学 网络空间安全学院

leimin@bupt.edu.cn

LSB隐写的特点

- 研究最早
- 算法简单
- 隐藏量大
- 应用广泛

LSB隐写的原理

- 位平面与视觉效果的关系
- 隐写技术——替换

原图

隐写后图像

LSB隐写步骤

- 将秘密信息转化为比特流
- 将比特流进行加密或置乱（用密钥）
- 逐行/或逐列/或随机游走的方式替换载体图像的最低比特位
- 接收者提取最低比特位，恢复秘密信息

思考

- 特征分析法对LSB隐写有效吗?
  - 隐写软件现有版本已经逐渐去除特征码
- 通过感观分析能够检测LSB隐写吗?
  - 有效：最低比特平面不具有随机性
  - 一般情况，隐写前后感观质量不下降
- 统计分析对LSB隐写有效吗?

χ^2分析

- LSB方法：
- 如果秘密信息位与隐藏位置的像素灰度值的最低比特位相同，不改变原始载体
- 反之，则改变灰度值的最低位
  - 0010 0011<->0010 0010 35<->34
  - 2i<->2i+1

χ^2分析

- 约定：
  - q：一个像素被选中用于隐藏信息的概率；
  - $T_c[j], j = 0,1,2,\cdots,255$：载体图像中，值为$j$的像素个数；
  - $T_s[j], j = 0,1,2,\cdots,255$：隐写图像中，值为$j$的像素个数；
- 假设：
  - 秘密消息中比特0和1随机分布；
  - $T_c[2i]$个值为$2i$的像素中，有$\frac{q}{2}T_c[2i]$个像素的最低比特与消息相同，不需要修改；

χ^2分析

- 假设：
  - 有$\frac{q}{2}T_c[2i]$个像素最低比特与消息不同，像素值变为$2i+1$；
  - 类似地，值为$2i+1$的像素中，有$\frac{q}{2}T_c[2i+1]$个像素最低比特与消息不同，像素值变为$2i$;
- 可得：
  - $E\{T_S[2i]\} = \left(1-\frac{q}{2}\right)T_c[2i] + \frac{q}{2}T_c[2i+1]$
  - $E\{T_S[2i+1]\} = \left(1-\frac{q}{2}\right)T_c[2i+1] + \frac{q}{2}T_c[2i]$

χ^2分析

- 当$q = 1$时：
  - $E\{T_S[2i]\} = E\{T_S[2i+1]\}$
  - $= 0.5\{T_c[2i] + T_c[2i+1]\}$
  - $= 0.5\{T_s[2i] + T_s[2i+1]\}$
  - 即，对于隐写图像来说，
  - 值为$2i$的像素个数的观测值为：$T_s[2i]$
  - 值为$2i$的像素个数的理论值$\overline{T_s}[2i]$为：$0.5\{T_s[2i] + T_s[2i+1]\}$
  - 当$q = 1$，这两者趋于相等。

χ2分析——值对翻转统计效果示例

- 在测试图像的所有最低位上嵌入秘密信息

χ2分析——值对翻转统计效果示例

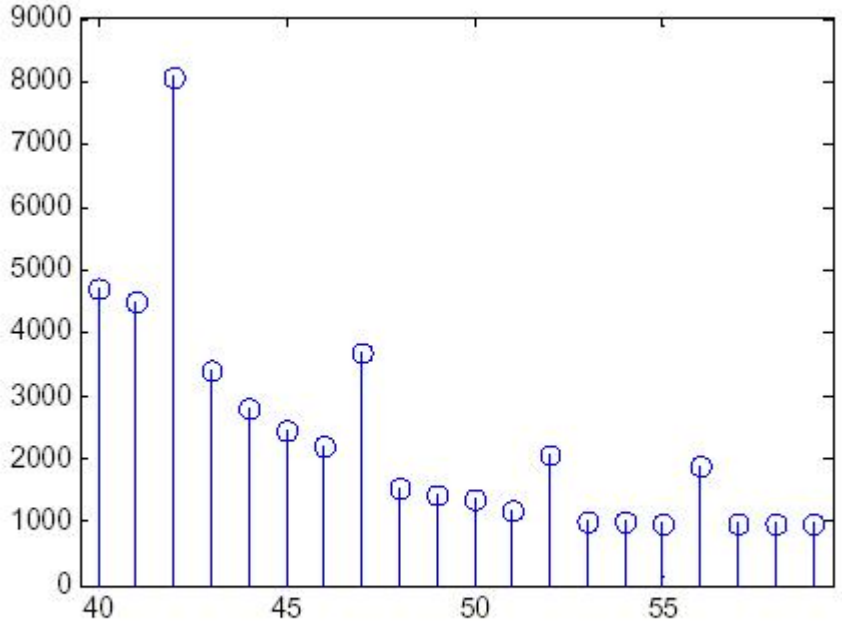


图 3.2.2 原始图象 Man 的灰度直方图局部

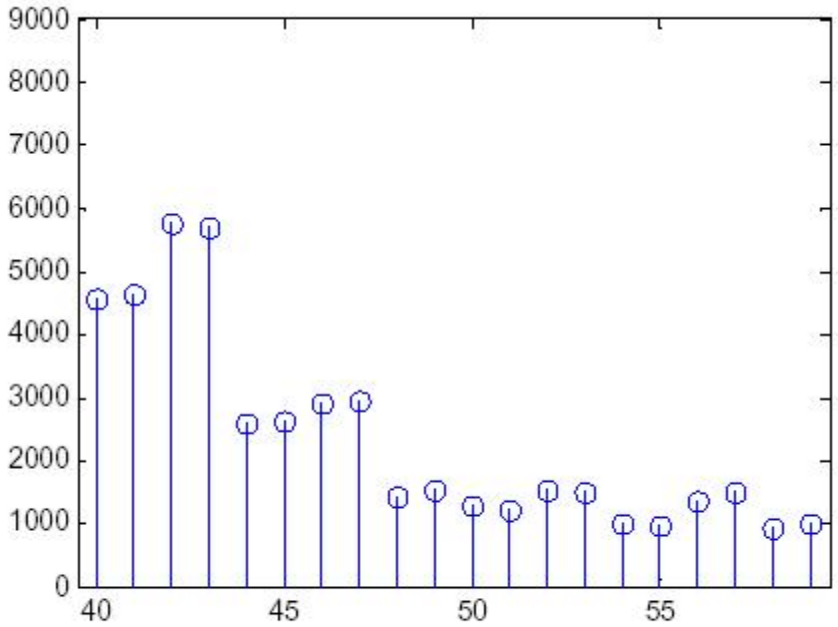
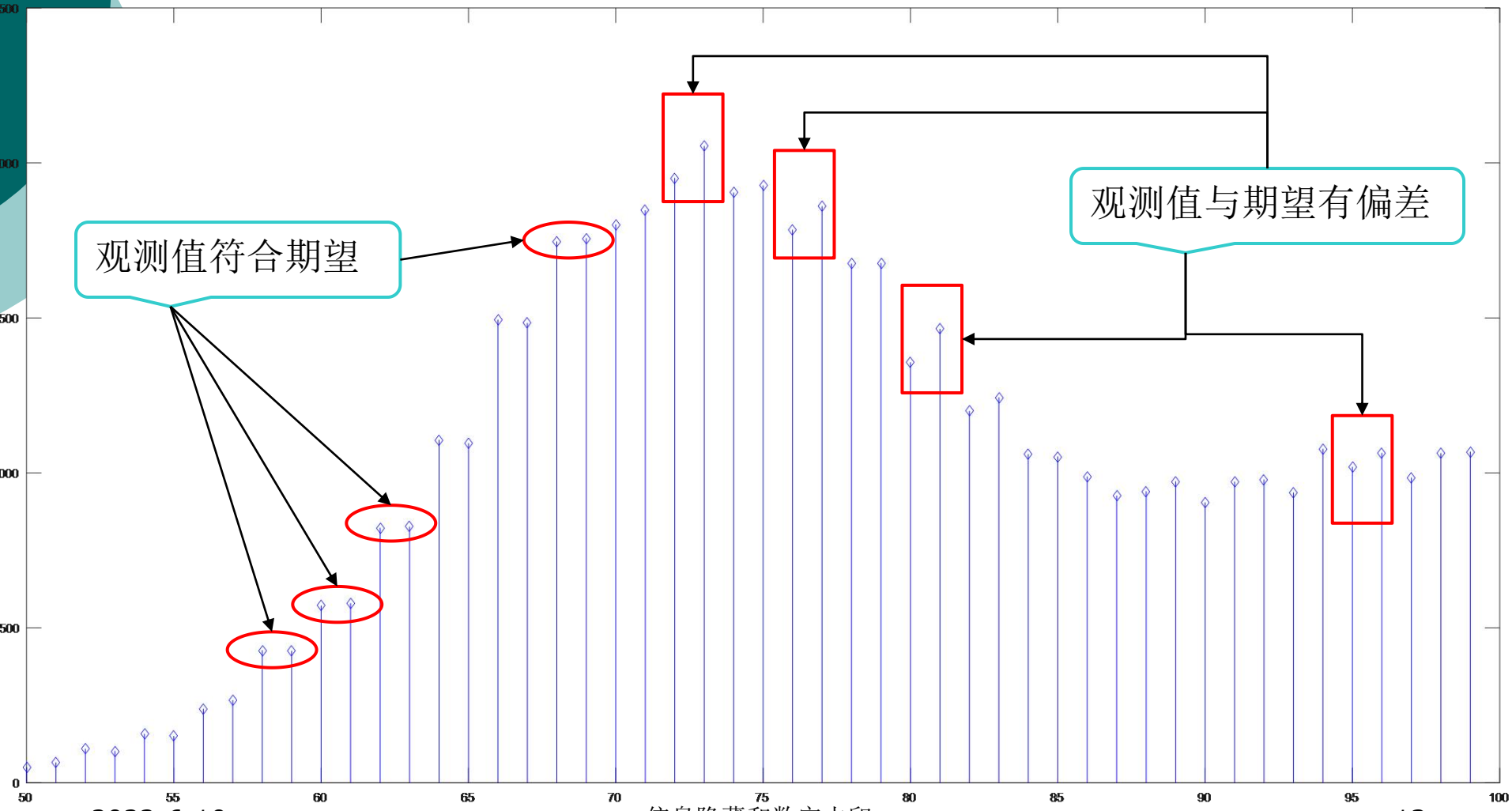


图 3.2.3 密写图象 Man 的灰度直方图局部

χ^2分析

- 结论：
  - 如果图像LSB隐写，那么$\overline{T_s}[2i]$与$T_s[2i]$一致。
- 问题：
  - $\overline{T_s}[2i]$与$T_s[2i]$的关系如何，可认为一致?

χ^2分析——$\overline{T_s}[2i]$与$T_s[2i]$



χ^2分析

- 卡方检验：
  - 如果图像LSB隐写，那么$\overline{T_s}[2i]$与$T_s[2i]$一致。
  - 可以用卡方检验来检测$\overline{T_s}[2i]$与$T_s[2i]$的一致性。
  - 由卡方检验原理可知，统计量
  - $$s = \sum_{i=1}^{k} \frac{(T_s[2i] - \overline{T_s}[2i])^2}{\overline{T_s}[2i]}$$
  - 服从自由度为$k-1$的卡方分布（χ^2分布）。

χ^2分析

- 隐写分析:
  - 计算待检测图像统计量s，s的值越小，意味$\overline{T_s}[2i]$与$T_s[2i]$越一致，也就是说待检测图像是隐写图像的概率越高；
  - 反之，s的值越大，意味$\overline{T_s}[2i]$与$T_s[2i]$差异越大，也就是说待检测图像是隐写的概率越低；
  - 通常计算p值，$p(s) = P(\chi \geq s), \chi \sim \chi^2(k-1)$来判别。
  - 如果图像没隐写，s很大，$p(s)$近似于0；
  - 实际应用中，$p(s) > \alpha$，即认为图像包含秘密信息。

实验结果

- 对灰度图像的上半部分进行LSB隐写，计算p值

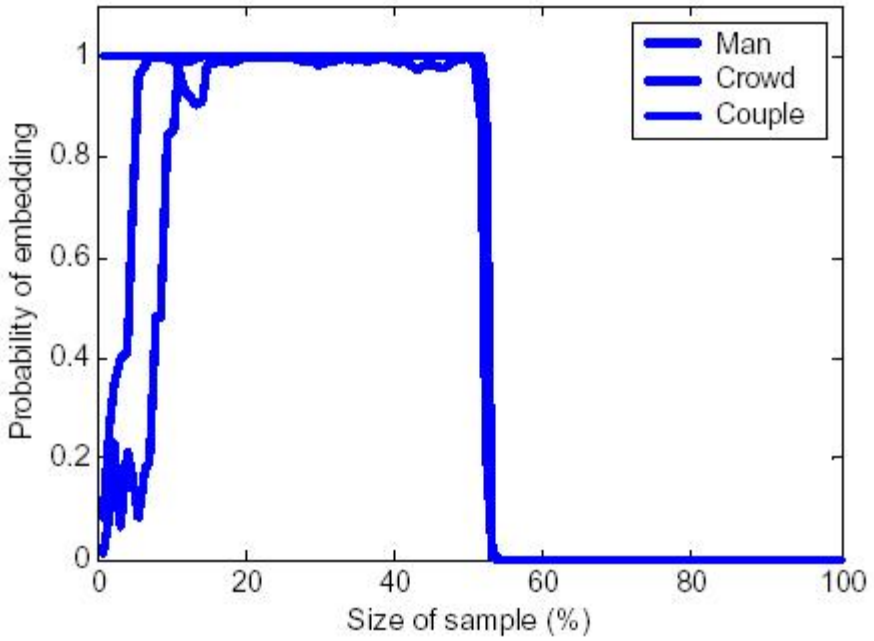


图 3.2.4　对三幅密写图象进行χ^2统计分析的结果。横坐标表示分析区域占整幅图象的比例，纵坐标表示密写可能性p的计算结果。

存在的问题

- 在下述情况下，卡方检测难以奏效
  - 不是连续嵌入
  - 隐写率较低

问题

- 根据卡方检测的原理，如何改进算法使其能够抵抗卡方分析?

直方图补偿隐写

- χ^2法关键：隐写后直方图改变
- 为提高隐写的安全性，设计的隐写算法要保持直方图不改变
- 对隐写后的图像进行额外操作，补偿直方图失真

小结

- 隐写分析（Steganalysis）
  - 判定载体是否隐写，隐写率，提取秘密信息
- 隐写分析方法
  - 感观分析，特征分析，统计分析，通用分析
- 卡方分析
  - 直方图统计特性变化
  - 灰度值为2i和2i+1的像素出现频率趋于相等
  - 隐写分析的结果反过来促进隐写技术的提高