07.1 基于LSB的隐写与隐写分析

钮心忻、杨榆、雷敏
北京邮电大学信息安全中心
yangyu@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?

χ2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

χ2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$qT_c[2i]$个像素被选中用于携带秘密信息；
- 其中大约一半，即 $\frac{q}{2}T_c[2i]$ 个像素的最低比特与消息相同，不需要修改；

χ2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：
  - $E\{T_S[2i]\}=\left(1-\frac{q}{2}\right)T_c[2i]+\frac{q}{2}T_c[2i+1]$
  - $E\{T_S[2i+1]\}=\left(1-\frac{q}{2}\right)T_c[2i+1]+\frac{q}{2}T_c[2i]$

χ2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$2i$的像素个数的期望（理论）值$\overline{T}_s[2i]$为：$0.5\{T_s[2i] + T_s[2i+1]\}$
  - 随着隐写率增加，$T_s[2i]$和$\overline{T}_s[2i]$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

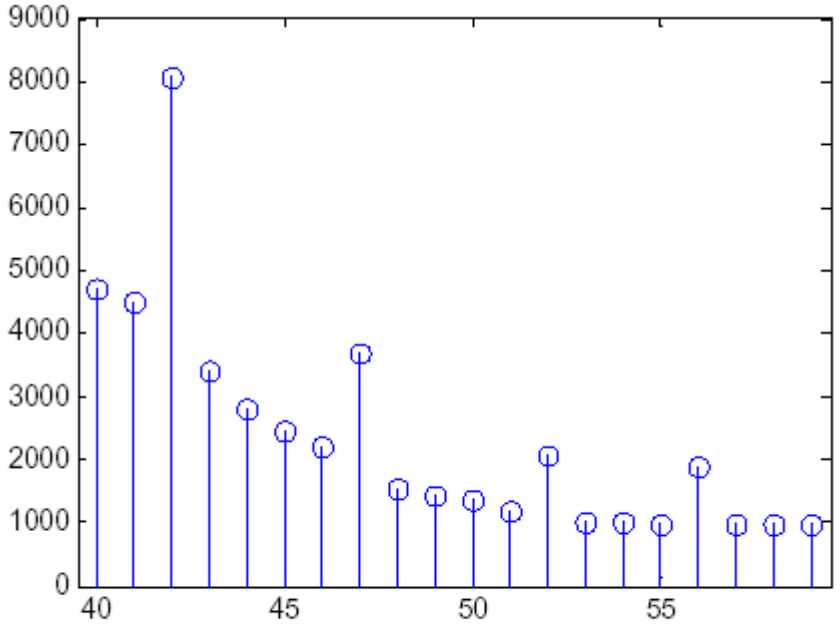


图 3.2.2 原始图象 Man 的灰度直方图局部

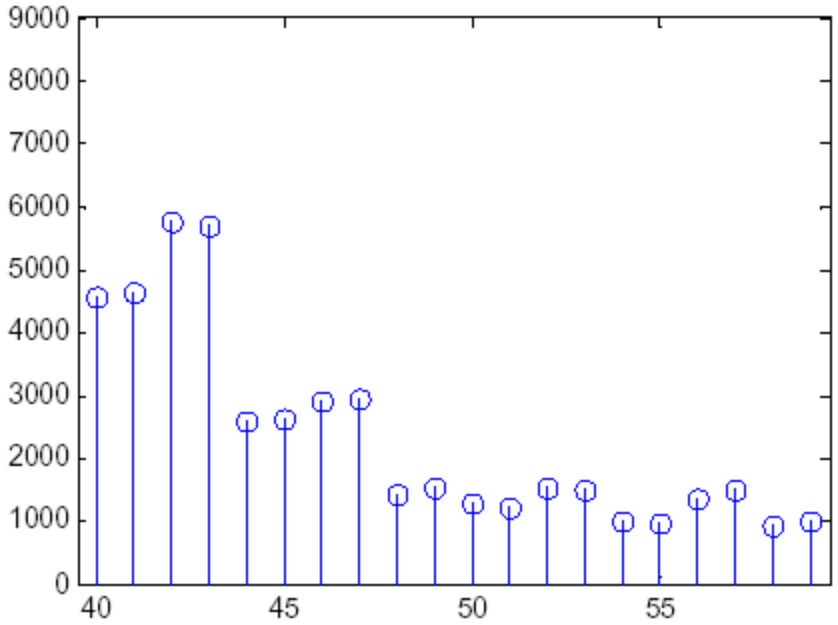
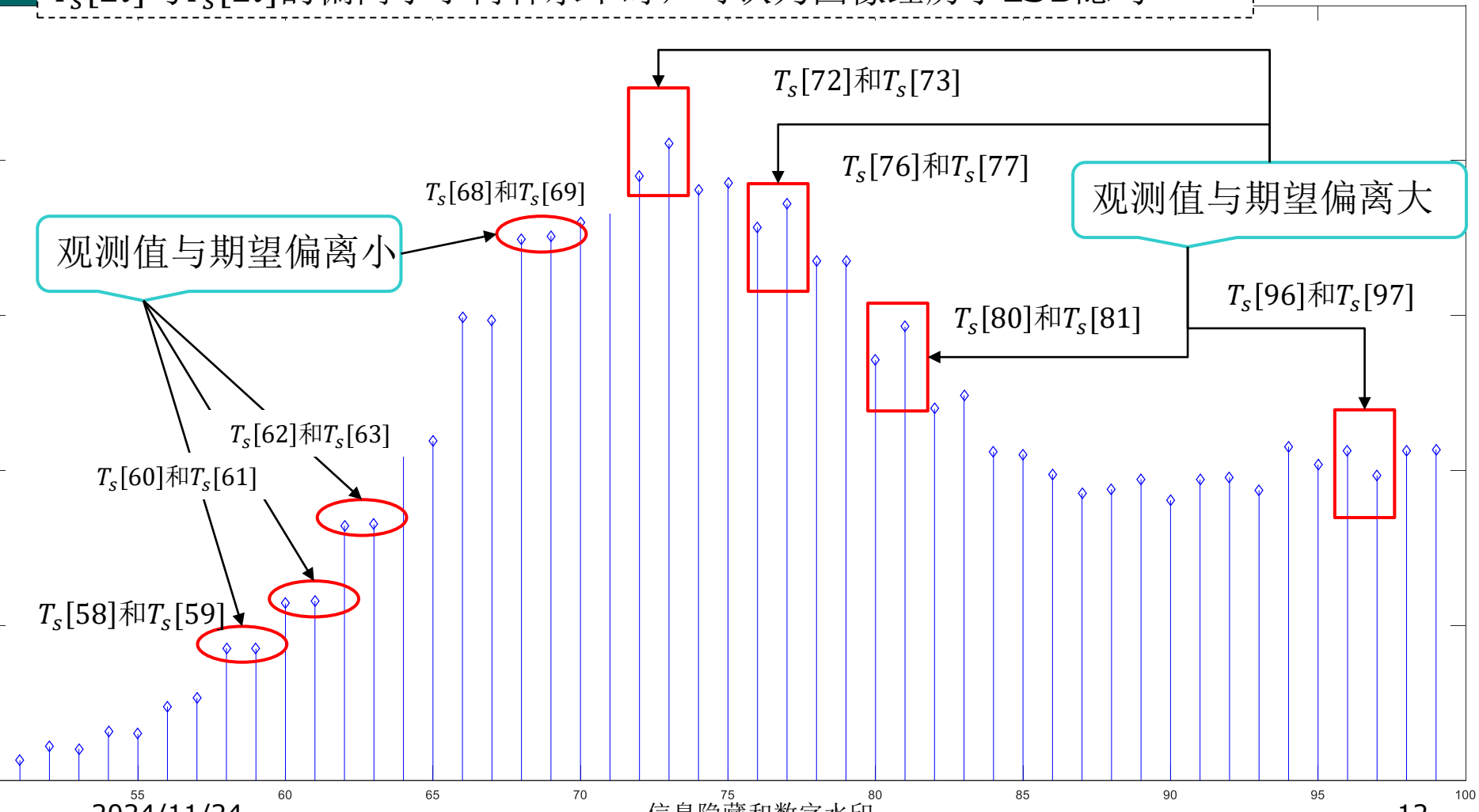


图 3.2.3 密写图象 Man 的灰度直方图局部

如果图像LSB隐写，那么$\overline{T}_s[2i]$与$T_s[2i]$趋于相等。

χ2分析——$\overline{T}_s[2i]$与$T_s[2i]$

$T_s[2i]$与$\overline{T}_s[2i]$的偏离小于何种水平时，可认为图像经历了LSB隐写？



χ2分析

卡方检验：

如果图像LSB隐写，那么$\overline{T_s}[2i]$与$T_s[2i]$趋于相等。可将其视为一个假设检验问题。

- 视$\overline{T_s}[2i]$与$T_s[2i]$为期望和实测值，假设图像隐写，则根据卡方检验，统计量（其中，$\overline{T_s}[2i] = 0.5\{T_s[2i] + T_s[2i+1]\}$）

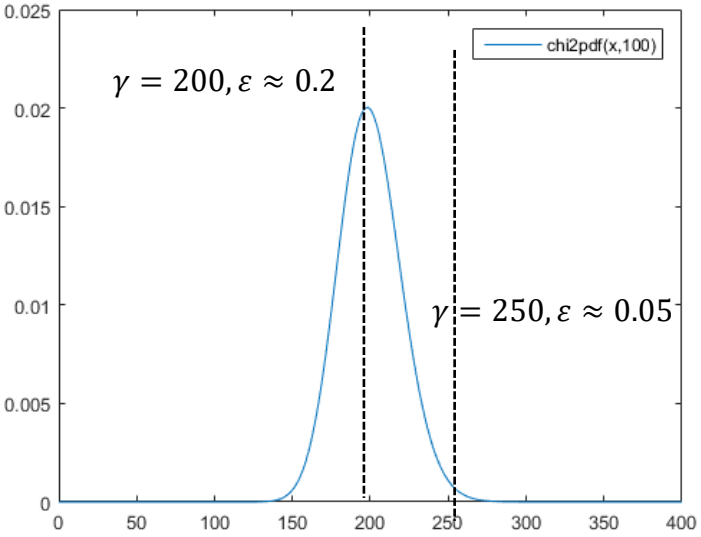
$$s = \sum_{i=1}^{k} \frac{(T_s[2i] - \overline{T_s}[2i])^2}{\overline{T_s}[2i]}$$

- 服从自由度为$k-1$的卡方分布（χ^2分布）。
- 若$s > \gamma$，则推翻假设，否则接受假设（即判定图像隐写）。
- γ由能够容忍的错误率决定。
  - 阈值γ越大，漏检率越低，即实际隐写、但期望和实测值差异过大的隐写图像也会被检出，但自然图像被误检为隐写图像的概率也随之提升，即虚警率升高。
  - 若可容忍的漏检率度为ε，则γ的选择应满足$\varepsilon = \Pr\{\chi^2_{k-1} > \gamma\}$

χ2分析

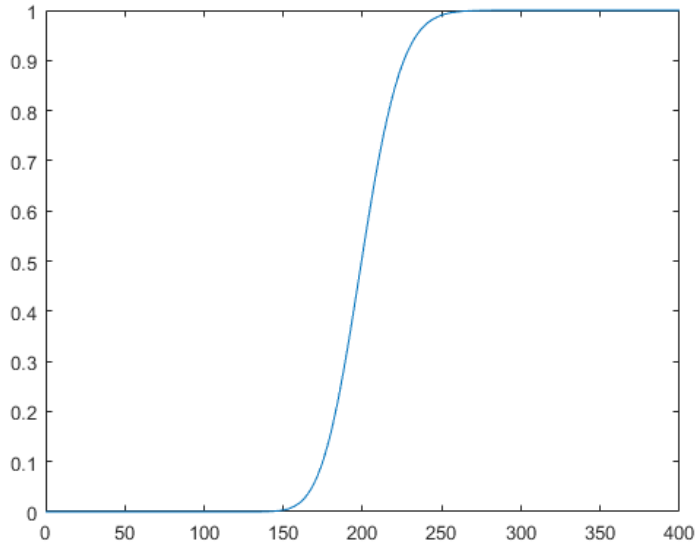
隐写分析：

- 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。（$\Pr\{\chi^2_{k-1} > \gamma\} = 1 - \Pr\{\chi^2_{k-1} \leq \gamma\}$）



chi2pdf(x,200)

自由度为200的服从卡方分布的随机变量的概率密度/质量函数



chi2cdf(x,200)

自由度为200的服从卡方分布的随机变量的累计分布函数

实验结果

- 对灰度图像的上半部分进行LSB隐写，计算p值

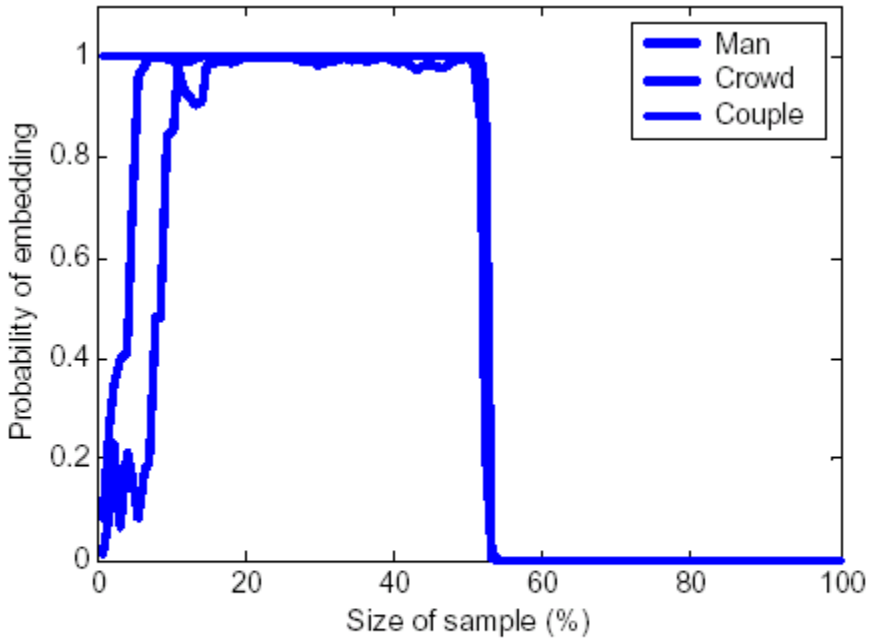


图 3.2.4　对三幅密写图象进行χ^2统计分析的结果。横坐标表示分析区域占整幅图象的比例，纵坐标表示密写可能性p的计算结果。

演示

- 利用卡方检测没有隐写、隐写率为30%、50%、70%和100%的图像

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

- χ2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

直方图补偿隐写

- 设原图像灰度值为 j 的像素个数为 f_j
- 隐写后图像灰度值为 j 的像素个数为 h_j
- 隐写率为α
  - F_{2i}中携带了秘密信息的像素为α* F_{2i}
  - 约 α* F_{2i} /2个像素灰度值翻转为2i+1
  - 约 α* F_{2i+1} /2个像素灰度值翻转为2i

$$h_{2i} \approx f_{2i} - \frac{\alpha}{2}(f_{2i} - f_{2i+1})$$

$$h_{2i+1} \approx f_{2i+1} - \frac{\alpha}{2}(f_{2i+1} - f_{2i})$$

直方图补偿隐写

- 如果 $f_{2i} > f_{2i+1}$
- 隐写使灰度值为 2i 的像个数下降，灰度值为 2i+1 的像素个数上升
- 补偿方法
  - 将不含秘密信息的值为 2i+1 的像素值改为 2i
  - 不含秘密信息的灰度值为2i+1的像素个数>=隐写后增加的灰度值为2i+1的像素个数

$$(1-\alpha) f_{2i+1} \geq \frac{\alpha}{2}(f_{2i} - f_{2i+1}) \qquad \alpha \leq \frac{2 f_{2i+1}}{f_{2i} + f_{2i+1}}$$

直方图补偿隐写

- 特点
  - 隐写后直方图不再趋于相等，χ2法失效
  - 嵌入量降低：部分载体用于补偿

RS分析方法

- LSB隐写引入翻转的不对称。
  - 值对（2i, 2i+1）相互翻转，例如，（2,3），（120,121）…
  - 没有形如（2i, 2i-1）的像素值翻转操作，
  - 没有形如(2i+1, 2i+2）的像素值翻转操作。
- 直方图补偿等改进算法仍然保留了翻转不对称这一问题。
- 针对这一问题，RS隐写分析方法以“翻转的不对称性”为切入点进行分析检测。

RS分析方法

- **图像统计特性的描述——空间相关性。**
- 翻转操作的分类及其对空间相关性的影响。
- 二次隐写及翻转不对称性的检测。

RS分析方法

- 对图像分块，以Zigzag方式扫描排列成一个向量（x1,…,xn)
- 定义该图像块的空间相关性

$$f\left(x_1, x_2, \cdots, x_n\right) = \sum_{i=1}^{n-1} \left| x_i - x_{i+1} \right|$$

- *f*越小，说明相邻像素之间变化越小，图像块的空间相关性越强

RS分析方法

- 图像统计特性的描述——空间相关性。
- **翻转操作的分类及其对空间相关性的影响**。
  - 三种翻转操作（函数）；
  - 空间相关性指标：正常/异常块及其比例；
  - 翻转操作对自然图像的影响；
  - 翻转操作对隐写图像的影响。
- 二次隐写及翻转不对称性的检测。

RS分析方法

定义翻转函数

记F_1为2i与2i+1的相互变化关系 $F_1(x)=\begin{cases}x+1, if\ x\%2==0\\x-1,, if\ x\%2==1\end{cases}$

- 0−1，2−3，。。。

- 记F_{-1}为2i-1与2i的相互变化关系 $F_{-1}(x)=\begin{cases}x-1, if\ x\%2==0\\x+1,, if\ x\%2==1\end{cases}$
  - 1−2，3−4，。。。
- 记F_0为不变关系 $F_0(x)=x$

RS分析方法

- LSB隐写可以用翻转函数描述
  - 秘密比特与载体LSB比特相同时，用F_0翻转
  - 秘密比特与载体LSB比特不同时，用F_1翻转

$$LSB(x_i) = \begin{cases} F_0(x_i), if\ x_i \& 0x01 = m_i \\ F_1(x_i), if\ x_i \& 0x01 \neq m_i \end{cases}$$

RS分析方法

- 图像统计特性的描述——空间相关性。
- **翻转操作的分类及其对空间相关性的影响。**
  - 三种翻转操作（函数）；
  - 空间相关性指标：正常/异常块及其比例；
  - 翻转操作对自然图像的影响；
  - 翻转操作对隐写图像的影响。
- 二次隐写及翻转不对称性的检测。

RS分析方法

- 图像分成大小相同的图像块
- 计算空间相关性函数*f*值
- 对图像块应用翻转函数，相当于在图像上叠加了噪声，一般情况下，图像相关性会被迫坏。
- 翻转后，若图像块相关函数*f*值增大，说明空间相关性减弱，像素起伏程度增加，则称该图像块是正常的（Regular）。
- 反之，则称该图像块是异常的（Singular）。

RS分析方法

- 对每个图像块应用**非负翻转**（F_1和F_0）
  - 计算像素起伏程度增加的图像块的比例，记为R_M
  - 计算像素起伏程度减小的图像块的比例，记为S_M
  - $R_M + S_M \leq 1$

RS分析方法

- 对每个图像块应用**非正翻转**（F_{-1}和F_0）
  - 计算像素起伏程度增加的图像块的比例，记为R_{-M}
  - 计算像素起伏程度减小的图像块的比例，记为S_{-M}
  - $R_{-M} + S_{-M} <= 1$

RS分析方法

- 图像统计特性的描述——空间相关性。
- **翻转操作的分类及其对空间相关性的影响**。
  - 三种翻转操作（函数）；
  - 空间相关性指标：正常/异常块及其比例；
  - 翻转操作对自然图像的影响；
  - 翻转操作对隐写图像的影响。
- 二次隐写及翻转不对称性的检测。

RS分析方法

- 对于自然图像，从统计上说，非负翻转或非正翻转会同等程度增加图像块的混乱程度
  - R_M近似等于R_{-M}
  - S_M近似等于S_{-M}
- 翻转会破坏图像块的空间相关性，一般情况下
  - R_M会大于S_M
  - R_{-M}会大于S_{-M}

RS分析方法

- 图像统计特性的描述——空间相关性。
- **翻转操作的分类及其对空间相关性的影响。**
  - 三种翻转操作（函数）；
  - 空间相关性指标：正常/异常块及其比例；
  - 翻转操作对自然图像的影响；
  - 翻转操作对隐写图像的影响。
- 二次隐写及翻转不对称性的检测。

RS分析方法

- 对于LSB隐写图像，则采用非负翻转和非正翻转的结果有明显不同
- 设原图隐写率为α，即：图像中有$\alpha/2$的像素应用了F_1翻转
- 对其应用非负翻转时，设其中F_1翻转的比例为β

RS分析方法

- 则非负翻转后有三类像素
  - 没有被翻转
    - 灰度值未变，像素比例为$(1-\alpha/2)(1-\beta)$
  - 经历一次翻转
    - 灰度值变化1，像素比例为：
    - $(1-\alpha/2)\beta+\alpha/2(1-\beta)=\alpha/2+\beta-\alpha\beta$
  - 经历二次翻转
    - 灰度值回到原始值，像素比例为$\alpha\beta/2$

隐写像素比例	隐写灰度值变化比例	翻转比例	不变比例	F1比例	F0比例
α	$\alpha/2$	$\alpha/2$	$1-\alpha/2$	β	$1-\beta$

RS分析方法

- 相当于在原图像上有$\alpha/2+\beta-\alpha\beta$像素被F1翻转，即比隐写图像增加了$(1-\alpha)\beta$的像素被翻转。
- $(1-\alpha)\beta$ 随α增大而减小，意味着：R_M与S_M的差距随α增大而减小。
- 当$\alpha=1$时，R_M与S_M近似相等。

RS分析方法

- 如果对隐写图像进行非正翻转，也有三类像素
  - 没有翻转的
  - 经历一次翻转的
  - 经历二次翻转的
    - F_1和F_{-1}，像素值变化为2，两次翻转不会抵消
- 所以，R_{-M}与S_{-M}的差距不会随α增大而减小

RS分析方法

- 关键结论
  - 对自然图像，非正翻转和非负翻转造成图像同等程度的混乱
    - R_M近似等于R_{-M}
    - S_M近似等于S_{-M}
  - 对于隐写图像
    - R_M 和S_M 的差距随隐写率的增大而减小
    - R_{-M} 和S_{-M}的差距不会随隐写率的增大而减小

实验

- 对Lena图像进行LSB隐写，在不同隐写率的条件下计算R_M、S_M、R_{-M}和S_{-M}

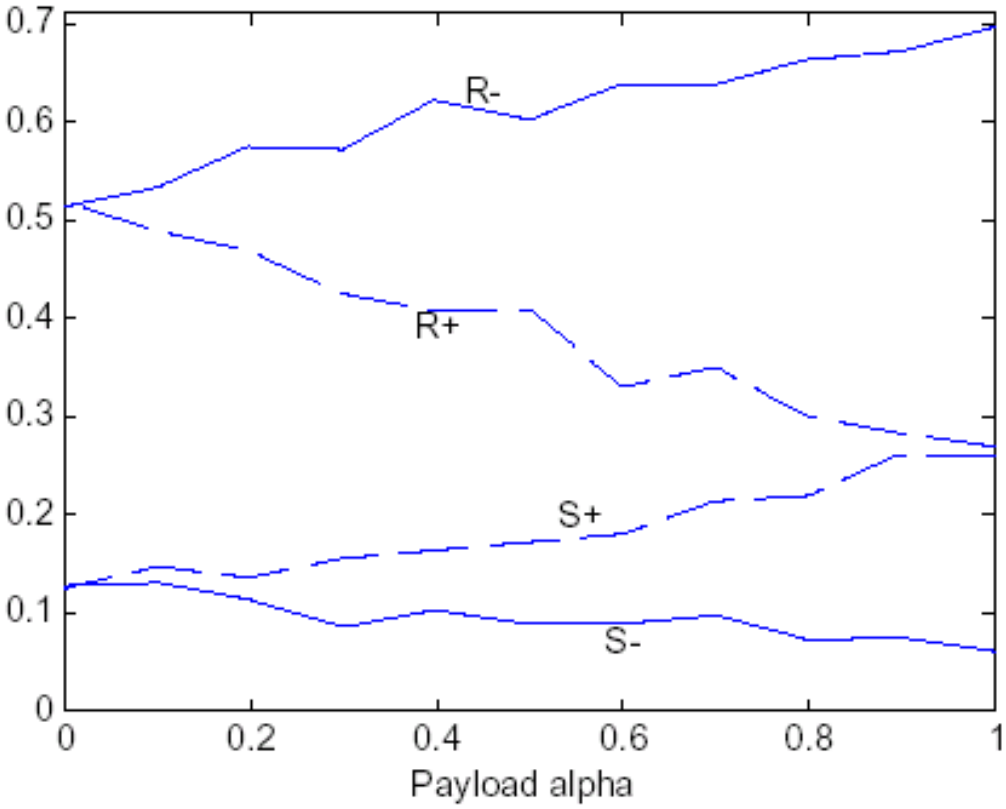


图 3.2.8 不同密写率时的R_M、S_M、R_{-M}、S_{-M}

RS分析方法

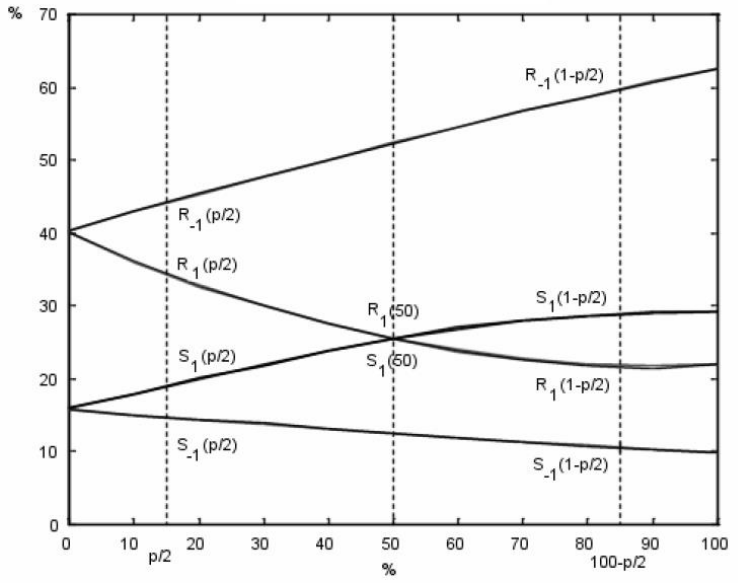
- 检测时：
  - 对待检测图像，进行非负翻转和非正翻转，计算R_M、S_M、R_{-M}和S_{-M}
  - 如果$R_{-M}-S_{-M}$显著大于R_M-S_M，则认为图像经过隐写

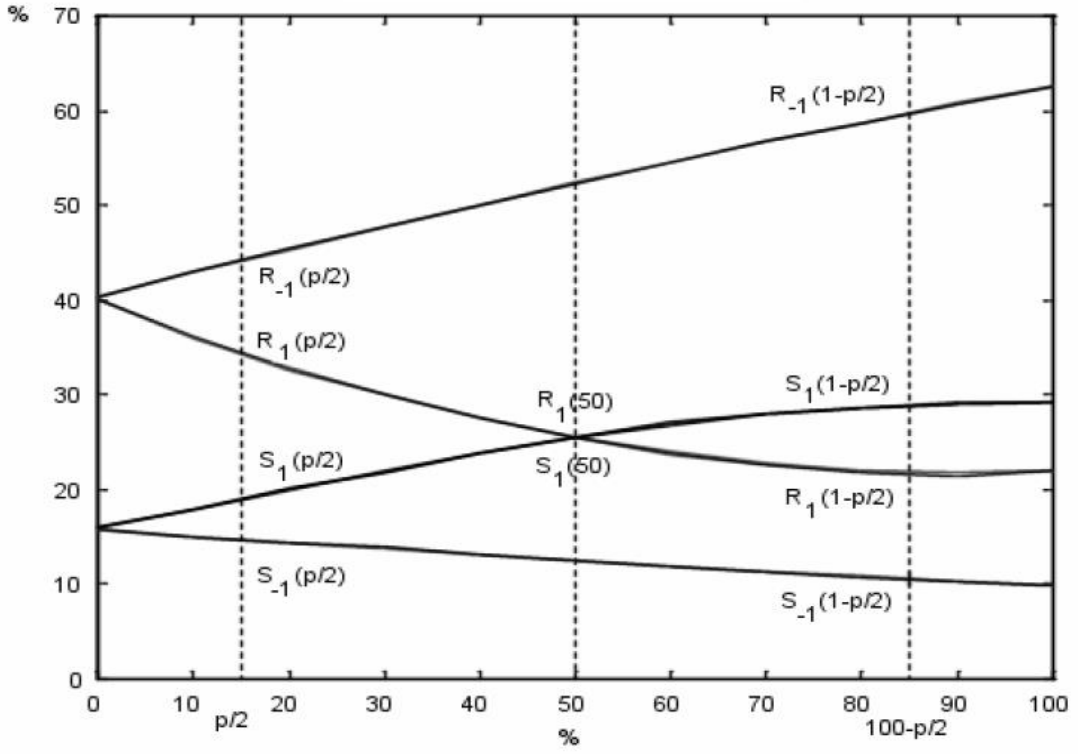
RS分析方法

- 图像统计特性的描述——空间相关性。
- 翻转操作的分类及其对空间相关性的影响。
  - 三种翻转操作（函数）；
  - 空间相关性指标：正常/异常块及其比例；
  - 翻转操作对自然图像的影响；
  - 翻转操作对隐写图像的影响。
- **二次隐写及翻转不对称性的检测**。

RS分析方法

- 设待检测图像嵌入率为p，则约有p/2的像素发生了翻转，计算此时的一组R、S值
- 翻转所有像素，则约有1-p/2的像素发生了翻转，再次计算R、S值





解方程：

$$2(d_1+d_0)z^2+(d_{-0}-d_{-1}-d_1-3d_0)z+d_0-d_{-0}=0$$

$$d_0=R_M\left(p/2\right)-S_M\left(p/2\right),d_1=R_M\left(1-p/2\right)-S_M\left(1-p/2\right)$$

$$d_{-0}=R_{-M}\left(p/2\right)-S_{-M}\left(p/2\right),d_{-1}=R_{-M}\left(1-p/2\right)-S_{-M}\left(1-p/2\right)$$

$$p=z/(z-0.5)$$

RS分析法

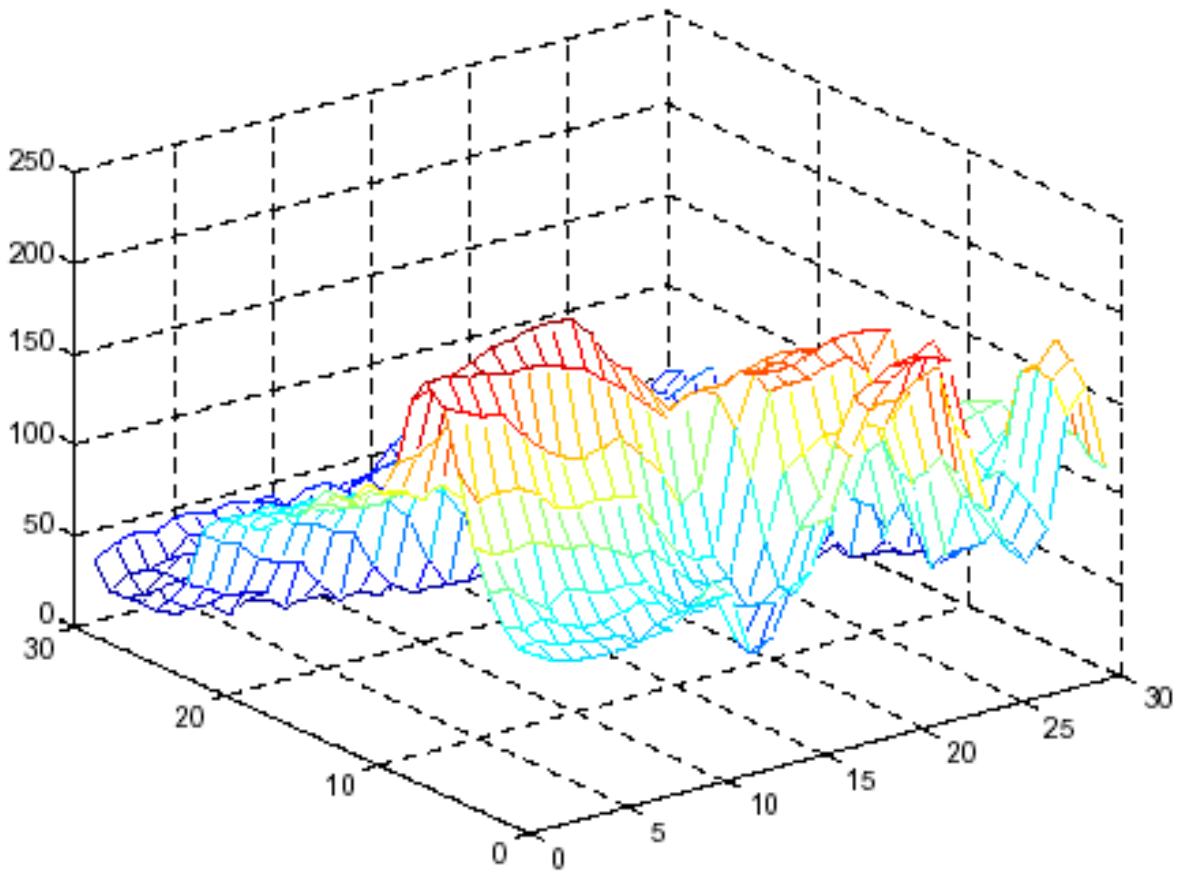
- 已知像素块如下，请尝试使用RS分析法判断像素块隐写的可能性。

8	9	10	9
9	10	11	12
10	11	12	11
9	10	11	10

GPC分析法

- 仍然是利用相邻像素的相关性进行隐写分析
- 把图像像素看成三维空间的点，构成一个网格

GPC分析法



GPC分析法

- 考虑两个平行于XY平面的平面簇
  - 平面簇P0由z=1.5, 3.5, 5.5,…, 255.5组成
  - 平面簇P1由z=0.5, 2.5, 4.5, …,254.5组成
- 令图像的三维曲面穿越平面簇P0的次数为N0
- 令图像的三维曲面穿越平面簇P1的次数为N1

GPC分析法

- 自然图像
  - N0近似等于N1
- LSB隐写图像
  - 载体数据在2i和2i+1之间互变
  - 不会穿越平面簇P0，但会穿越平面簇P1
  - N0不变，N1增大
- 令R＝N1/N0，如果R大于阈值，认为是隐写图像

GPC分析法

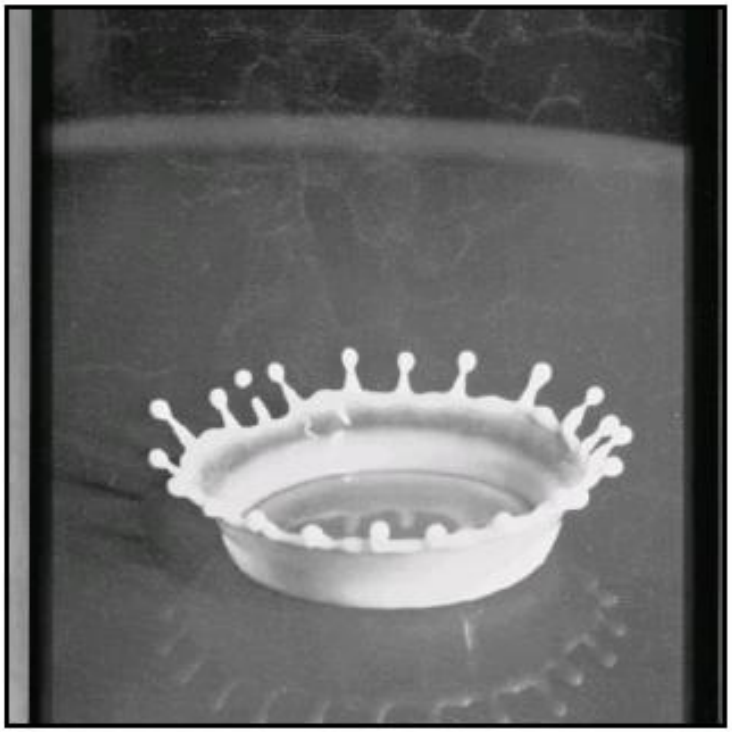
- 例如
  - 设有三个灰度值为4、2、4的相邻像素
  - 使用LSB嵌入1、0、1
  - 考察原始图像N1/N0，和隐写图像N1/N0
  - (4,2)穿越PO中的z=3.5平面，穿越P1中的z=2.5平面，(2,4)相同，所以N1=2，N0=2，R=1

GPC分析法

- 例如
  - 设有三个灰度值为4、2、4的相邻像素
  - 使用LSB嵌入1、0、1
  - 考察原始图像N1/N0，和隐写图像N1/N0
  - 隐写后，灰度值变为5、2、5
  - (5,2)穿越PO中的z=3.5平面，穿越P1中的z=2.5,4.5平面，(2,5)相同，所以N1=4，N0=2，R=2

实验结果

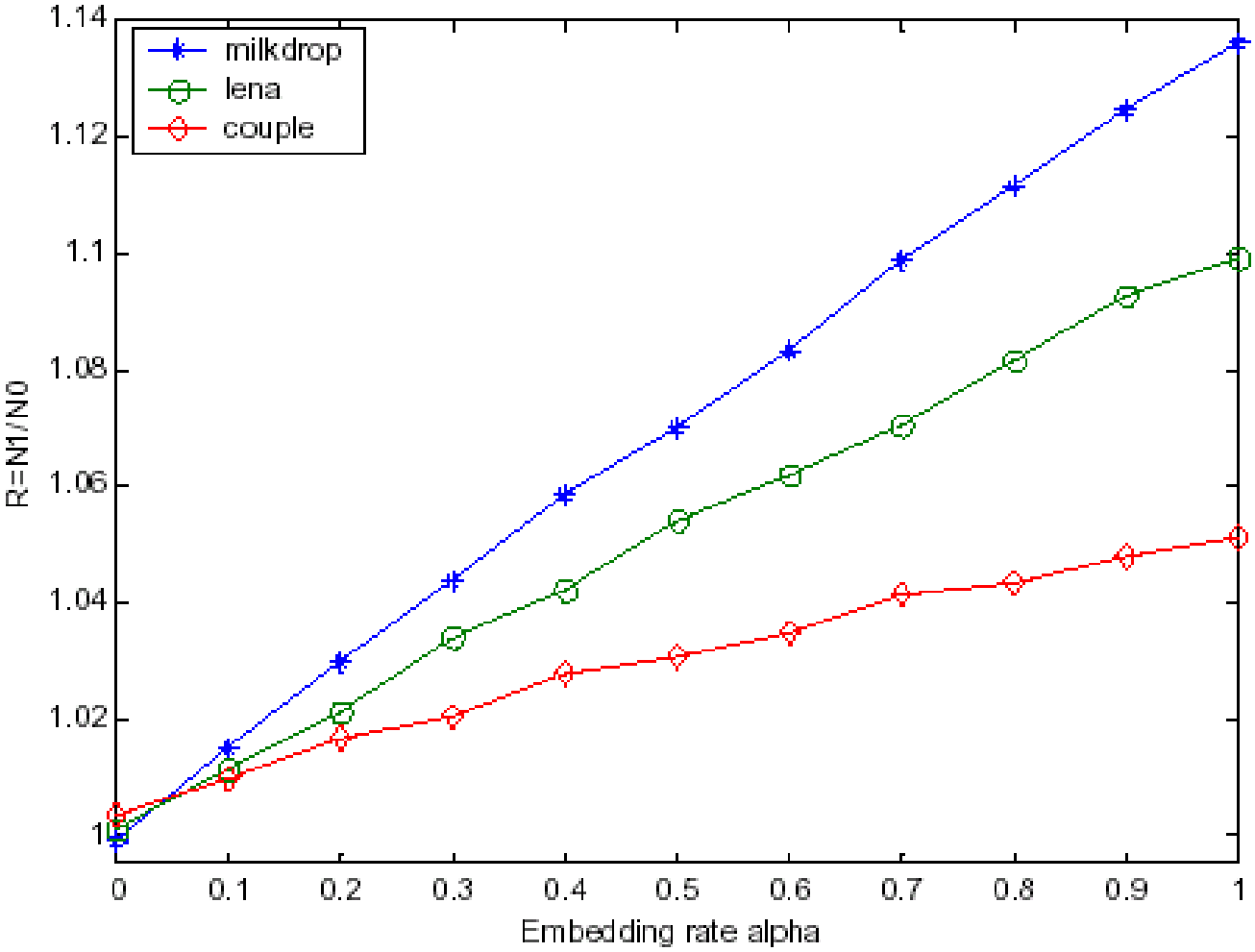
- 三幅图像：Lena，Milk Drop，Couple



(a) Milk Drop

(b) Couple

GPC分析法


milkdrop
lena
couple
R=N1/N0
Embedding rate alpha
1.14
1.12
1.1
1.08
1.06
1.04
1.02
1
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

GPC分析法

- 特点
  - 图像本身越平滑，该检测方法越敏感

思考

- 直方图补偿隐写能抵抗RS和GPC分析吗?
  - 无法抵抗RS分析和GPC分析（检测2i与2i+1、2i+1与2i+2之间的不对称性）

改进的LSB隐写

- 抵抗RS分析和GPC分析
- 修改LSB方法
  - 不仅仅在 2i和2i+1间翻转
  - 2i可变为 2i-1，2i+1 可变为2i+2

改进的LSB隐写

- 设秘密信息位为w，对应隐藏该位的像素灰度值为$x(i, j)$
  - 如果w 与$x(i, j)$的最低比特位相同，即$w = x(i, j) \bmod 2$，那么不改变原始数据
  - 当w 与$x(i, j)$的最低比特位不同，即$w \neq x(i, j) \bmod 2$ 时，计算

$$T = \sum_{u=i-1}^{i+1} \sum_{v=j-1}^{j+1} x(u, v) - 9 \cdot x(i, j)$$

改进的LSB隐写

- 对$x(i,j)$作如下调整

$$x(i,j)=\begin{cases} x(i,j)-1 & , \quad \text{if } T\le 0, 0<x(i,j)<255 \\ x(i,j)+1 & , \quad \text{if } T>0, 0<x(i,j)<255 \\ x(i,j)-1 & , \quad \text{if } x(i,j)=255 \\ x(i,j)+1 & , \quad \text{if } x(i,j)=0 \end{cases}$$

- 根据T确定增减的目的是使隐写不过分影响相邻像素之间的相对关系

改进的LSB隐写

- 可能会影响多个比特位
- 提取时：将最低比特位取出即可

改进LSB隐写

- 已知像素块如下，若要藏入秘密比特序列：1,0,1,0,0,1,1,1,0，则像素块变为：

4	5	4
6	5	6
7	6	5

改进的LSB隐写

- 抗RS分析性能：
  - 隐写时，约有一半像素的最低比特位与秘密信息相同而不发生变化，另一半像素灰度值会发生变化
  - 在发生变化的像素中，又约有一半像素的灰度值做了F1翻转，另一半做了F-1翻转
  - RS分析失效
- 抗GPC分析性能：
  - 修改像素值时，穿越P0和P1平面簇的可能性相同
  - GPC分析失效

改进的LSB隐写

- 抗卡方分析性能：
  - 灰度为 j 的像素中会有大约一半不变，大约四分之一变为j+1，剩余大约四分之一变为 j-1
  - 不会造成隐写后直方图趋于相等
  - χ2法失效

最小直方图失真隐写

- 尽量保持F_1和F_{-1}翻转的平衡
- 尽量保持直方图不变

最小直方图失真隐写

- 设原始图像灰度值为 j 的像素共有 f_j 个
- g_j: 需要加1或减1的像素个数
- x_j: 灰度值被减1的像素个数
- g_j-x_j: 灰度值被加1的像素个数
- 则新产生的值为 j 的像素个数为

$$g'_j = x_{j+1} + (g_{j-1} - x_{j-1})$$

最小直方图失真隐写

- 约束条件：
  - 1、直方图失真最小

$$d = \|\mathbf{g}' - \mathbf{g}\| = \sqrt{\sum_{j=0}^{255} (g'_j - g_j)^2}$$

  - 2、 F_1和F_{-1}翻转的平衡

$$\sum_{j=2i} x_j + \sum_{j=2i+1} (g_j - x_j) = \sum_{j=2i+1} x_j + \sum_{j=2i} (g_j - x_j)$$

- 解矩阵方程，得到近似最优解

小结

- 隐写分析（Steganalysis）
  - 判定载体是否隐写，隐写率，提取秘密信息
  - Stego-only attack; Known-cover attack; Known-message attack; Chosen-stego attack; Chosen-message attack
- 隐写分析方法
  - 感观分析，特征分析，统计分析，通用分析
- 隐写分析的结果反过来促进隐写技术的提高

小结

- 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
- RS分析
  - 利用图像空间相关性进行隐写分析
  - 对自然图像，非负和非正翻转同等程度地增加图像的混乱程度
  - 对隐写图像，R_m-S_m随隐写率的增大而减小
  - 对隐写图像，R_{-m}-S_{-m}没有上述关系

小结

- GPC分析
  - 利用图像空间相关性进行隐写分析
  - 自然图像，N0近似等于N1
  - 隐写图像，N1随隐写率增大而增加
- 改进算法
  - 直方图补偿隐写
  - 改进LSB隐写
  - 最小直方图失真隐写

练习

1. 攻击者只有隐蔽载体，想从中提取秘密信息，属于_____；攻击者不但截取了掩蔽载体，还获得了该掩蔽载体对应的原始载体，属于_____；攻击者利用隐写工具产生一系列掩蔽载体，分析其特征，以帮助隐写分析，属于_____。

A. Known-cover attack
B. Stego-only attack
C. Chosen-message attack
D. Known-message attack

练习

2 关于隐写分析，下列说法不正确的是：_____。

A. 设计图像隐写算法时往往假设图像中LSB位完全随机，实际使用载体的LSB平面的随机性并非理想，因此连续的空域隐藏很容易受到视觉分析攻击。

B. 感观分析的一个弱点是自动化程度差。

C. 隐写经常会改变原始载体的某些统计特征。通过分析待检测载体的统计特征，可以判断载体是否经过隐写。这种隐写分析方法称为特征分析法。

D. 通用隐写分析旨在设计与具体隐写算法无关的隐写分析方法。

练习

3 卡方分析的原理是：_____。

A. 利用图像空间相关性进行隐写分析

B. 非负和非正翻转对自然图像和隐写图像的干扰程度不同

C. 图像隐写后，灰度值为2i和2i+1的像素出现频率趋于相等

D. 图像隐写后，其穿越平面簇z=0.5、2.5、4.5。。。的次数增加

练习

4 关于RS分析，下列说法不正确的是：_____。

A. 对自然图像，非负和非正翻转同等程度地增加图像的混乱程度

B. 对隐写图像，应用非负翻转后，规则与不规则图像块比例的差值随隐写率的增大而减小

C. 对隐写图像，应用非正翻转后，R-m与S-m的差值随隐写率的增大而减小

D. RS分析和GPC分析都是针对灰度值在2i和2i+1间与在2i和2i-1间翻转的不对称性进行的

练习

5 下列关于改进算法的描述，不正确的是:

A. 最小直方图失真隐写算法在尽量保持F1和F-1翻转平衡的情况下，使直方图在隐写前后变化量尽可能小，可以抵抗卡方分析。

B. 直方图补偿隐写算法确保隐写后，直方图中2i和2i+1的频度不再趋于相等，因此可以抵抗RS分析。

C. 改进LSB隐写算法翻转像素灰度时，2i不仅可以变为2i+1，也可变为2i-1

D. 改进LSB隐写算法可以抵抗卡方、RS和GPC分析

解答

1. 攻击者只有隐蔽载体，想从中提取秘密信息，属于 Stego-only attack ；攻击者不但截取了掩蔽载体，还获得了该掩蔽载体对应的原始载体，属于 Known-cover attack ；攻击者利用隐写工具产生一系列掩蔽载体，分析其特征，以帮助隐写分析， 属于 Chosen-message attack。

A. Known-cover attack
B. Stego-only attack
C. Chosen-message attack
D. Known-message attack

解答

2　关于隐写分析，下列说法不正确的是：　C　。

A. 设计图像隐写算法时往往假设图像中LSB位完全随机，实际使用载体的LSB平面的随机性并非理想，因此连续的空域隐藏很容易受到视觉分析攻击。

B. 感观分析的一个弱点是自动化程度差。

C. 隐写经常会改变原始载体的某些统计特征。通过分析待检测载体的统计特征，可以判断载体是否经过隐写。这种隐写分析方法称为特征分析法。

D. 通用隐写分析旨在设计与具体隐写算法无关的隐写分析方法。

说明：特征分析的特征是指隐写软件在载体中留下的与秘密信息无关的特征。有的特征是URL地址等文本信息，有的特征是有规律的二进制串。

解答

3　卡方分析的原理是：　C　。

A. 利用图像空间相关性进行隐写分析

B. 非负和非正翻转对自然图像和隐写图像的干扰程度不同

C. 图像隐写后，灰度值为2i和2i+1的像素出现频率趋于相等

D. 图像隐写后，其穿越平面簇z=0.5、2.5、4.5。。。的次数增加

解答

4 关于RS分析，下列说法不正确的是：__C__。

A. 对自然图像，非负和非正翻转同等程度地增加图像的混乱程度

B. 对隐写图像，应用非负翻转后，规则与不规则图像块比例的差值随隐写率的增大而减小

C. 对隐写图像，应用非正翻转后，R-m与S-m的差值随隐写率的增大而减小

- RS分析和GPC分析都是针对灰度值在2i和2i+1间与在2i和2i-1间翻转的不对称性进行的

解答

5 下列关于改进算法的描述，不正确的是：B

A. 最小直方图失真隐写算法在尽量保持F1和F-1翻转平衡的情况下，使直方图在隐写前后变化量尽可能小，可以抵抗卡方分析。

B. 直方图补偿隐写算法确保隐写后，直方图中2i和2i+1的频度不再趋于相等，因此可以抵抗RS分析。

C. 改进LSB隐写算法翻转像素灰度时，2i不仅可以变为2i+1，也可变为2i-1

D. 改进LSB隐写算法可以抵抗卡方、RS和GPC分析

说明：补偿翻转像素沿用LSB方式，所以翻转之间的不对称性仍然存在，故而能被RS算法检测。