lsb随机隐写 c语言,3随机LSB替换隐写及RS检测方法.doc

转载

何为浮云 于 2021-05-24 04:03:28 发布 308 收藏 2
文章标签： lsb随机隐写 c语言

3 随机LSB替换隐写及RS检测方法

【实验目的】

设计并实现一种随机LSB替换隐写方法，并考察其抵抗卡方检测的能力；

实现RS检测方法，并考察其检测随机LSB替换隐写的能力；

设计其他可以检测随机LSB隐写的方法.

【实验环境】

Matlab7.1或以上版本；或者VC6.0；

BMP灰度图像

【实验原理及方法】

随机LSB替换隐写

记号：c表示嵌入过程中的原始灰度图像(载体)可用一个长为l(c)的序列来表示，可通过从左向右，从上到下将所有像素排列起来获得其中表示对应像素的灰度值，s表示嵌入秘密信息后的隐秘图像，也可看作长为的序列，m表示待嵌入的秘密消息，是一个长为的由组成的序列， l(c)，一般而言，。j表示图像的索引值。ji表示索引值的顺序排列cji表示第ji个载体元素k表示隐写密钥

LSB替换隐写

1) 在中根据密钥k生成伪随机嵌入路径，即选择个像素。

2) 对于的每一个像素，

3) 用秘密信息比特取代原灰度值的LSB，而高7位保持不变，修改后的图像即为。

LSB替换隐写提取根据密钥找到中嵌入信息的像素，抽出这些像素灰度值的LSB，排列后组成秘密信息。

间隔使用伪随机数发生器来生成一个伪随机序列k1, k2, …, kl(m)，k1个像素嵌入信息，第二步选择第k1,+k2个像素嵌入信息，以此类推，如图3.7所示。

图3.7 随机间隔示意

问题：

随机选位算法对于隐写软件设计非常重要，事实上有些隐写软件就是因为随机选位机制设计的不合理而被攻破。为了安全应如何设计随机间隔法？你能想到其他随机选位方法吗？

卡方检测方法能够检测随机LSB替换隐写码？

2．RS检测原理

RS方法是由Fridrich等人提出的，该方法适合于检测随机LSB替换隐写，可以比较精确地估计隐藏信息长度，它是基于统计隐写前后图像平滑度的变化来检测秘密信息的。

假定一幅载体图像具有M(N个像素，像素值属于一个集合P。如对8-bit灰度图像，P={0, 1, (, 255}。函数f(x1, x2, (, xn)描述了像素组G=(x1, x2, (, xn)的平滑度，具体定义为：

()

这个函数称为判别函数，用来描述像素组G的空间相关性。G中的噪声越多，函数f的值越大。LSB嵌入信息增加了图像的噪声，f的值也将随之增加。LSB替换隐写的嵌入过程可以用翻转函数来描述：

F1: 0 (1, 2 (3, …, 254 (255

F1具有下列性质：

FLSB(x) = F1(x) = x+1(2((x mod 2)

即改变灰度级 x 的LSB等同于对x应用翻转函数F1。

同时可定义一个对偶的概念，称作移位LSB 翻转函数：

F(1： (1 (0, 1 (2, 3 (4, …, 253 (254, 255 (256

则有：

F(1(x) = F1(x+1) (1

为了完整性，定义F0为自身置换，即

F0(x)=x

F1,F-1,F0统称为翻转函数。

对像素组G=(x1, x2, (, xn)，若f(F(G))>f(G)，称G是正则的；若f(F(G))

()

将图像分成许多大小相等的小图像块，对每个小块应用非负翻转，即M(1), M(2), …, M(n)为1或0，利用式()计算，考察图像的变化情况。用RM表示FM作用后正则图像块在所有图像块中所占的比例；SM表示FM作用后奇异图像块在所有图像块中所占的比例。如此，则有RM+SM≤1，类似地应用非正翻转(M(1), M(2), …, M(n))，这里M(i)为-1或0，可定义相应的R(M和S(M。

图 RS示意图

RS方法是根据大量的统计特性而得到的，Fridrich等人指出：和与信息嵌入比率p呈线性关系，和是信息嵌入比率p的二次曲线，如图所示。并且成立下述事实：

1) 如果待测图像没有经过LSB替换隐写，那么无论应用非负翻转还是非正翻转，从统计规律来看，会同等程度地增加图像块的混乱度，也就是说，RM (R(M，SM (S(M，而且RM >SM，R(M > S(M；

2) 如果待测图像是经过LSB替换隐写的，应用非负翻转和非正翻转之后的结果就会有明显差别。即：R(M (S(M >> RM(SM成立；

3) RM 和 SM 之间的差异随着信息嵌入比率的增加而趋近于0，即：RM (SM。

通过统计RM、SM 、R(M 和S(M在p/2和(1(p/2)处的值可建立如下方程：