# 基于相邻灰度值对互补嵌入的LSB匹配隐写改进算法

奚 玲 平西建 张 涛
(解放军信息工程大学 郑州 450002)

**摘 要** LSB匹配隐写具有嵌入量大、视觉隐蔽性高的优势,但采用LSB匹配隐写算法对于载密图像的灰度直方图有明显的平滑作用,因此攻击者可以基于直方图分析图像是否载密。通过研究LSB匹配算法对直方图产生影响的机理,提出一种基于相邻灰度值互补嵌入的LSB匹配改进算法。该算法利用匹配像素灰度值加减1对直方图的影响具有互补性的特点,以相邻灰度值匹配像素对为对象进行成对嵌入,有效地保持了直方图特性,极大地提高了算法的抗统计分析性能。

**关键词** LSB匹配,直方图,统计分析
**中图法分类号** TP309,TP391 **文献标识码** A

## Improved LSB Matching Steganographic Method Based on Complementary Embedding of Adjacent Intensity Pixels

XI Ling PING Xi-jian ZHANG Tao
(PLA Information Engineering University, Zhengzhou 450002, China)

**Abstract** LSB matching steganographic method has the advantage of large capacity and high invisibility, but the histogram of the stego image produced by this method is smoothened. Then attackers can detect whether the image has been changed. In this paper, an improved method was proposed. According to the complementary property of the random ±1 behavior, the improved method embeds most of the secrete bits in pixels with adjacent intensity. By the proposed method the cover image's histogram can be maintained in a considerable extend so as to make the stego image more difficult to be detected than LSB matching steganograpy.

**Keywords** LSB matching, Histogram, Statistic analyzer

## 1 引言

信息隐藏是互联网时代信息安全领域的重要研究内容之一。数字隐写和隐写分析是信息隐藏的两个相互促进、共同发展的方向。数字隐写研究如何将秘密信息隐藏到公开的数字媒体中,并以不引起第三方注意的方式进行传输,即隐蔽通信问题。而隐写分析的目的在于揭示媒体中隐蔽信息的存在性,阻断隐蔽通信。

LSB算法是出现最早的隐写算法,它通过用秘密信息取代载体数据的最低比特位来嵌入秘密信息。但传统LSB隐写算法产生的灰度直方图"值对"现象使攻击者能够使用统计分析的方法,例如 $\chi^2$ 分析[1]、RS分析[2]等,成功地判断图像中是否含有秘密信息。LSB匹配隐写针对传统LSB隐写存在的问题进行了改进。该方法通过随机加减1的嵌入修改方式,消除了传统LSB隐写算法在嵌入秘密信息时的奇偶性不对称,因而消除了载密图像直方图的"值对"现象,使利用这一特性进行攻击的分析算法失效。然而,随之而来的各种针对LSB匹配的隐写分析方法对LSB匹配隐写的安全性提出了挑战:质心法[3]、校准质心法[4]、局部极值法[5]等多种基于灰度直方图的分析算法都具有良好的性能。因此,要进一步提高安全性,保持隐写前后图像直方图的一致性是关键。目前一些以保持直方图特性为目的的改进LSB匹配隐写算法[6,7],以直方图的改变量控制每次嵌入修改的方向是加1还是减1,这些算法在一定程度上减小了直方图的改变。然而直方图是像素灰度值出现频率的统计特性,所以以此为基础的改进算法只能宏观调节隐写对直方图的影响,因此从直方图保持的角度来说,LSB匹配算法仍有改进空间。

本文通过研究LSB匹配算法对直方图产生影响的机理,提出一种基于相邻灰度值对互补嵌入的LSB匹配改进算法。该算法的思路不同于基于直方图改变量的保持算法,它利用相邻灰度值像素加减1对直方图影响的互补特性,将嵌入操作的对象由单个像素变为灰度值相邻的匹配像素对,从而有效地保持了直方图特性,提高了LSB匹配算法的抗统计分析性能。

## 2 对LSB匹配隐写算法的改进方案

### 2.1 LSB匹配隐写方法的直方图异常分析

文献[3]指出,LSB匹配隐写后,载密图像的灰度直方图

到稿日期:2009-10-10 返修日期:2010-01-19 本文受国家自然科学基金(60903221)资助。
奚 玲(1975—),女,博士生,主要研究方向为信息隐藏等,E-mail:bluesunshine_xl@sina.com;平西建(1953—),男,博士生导师,主要研究方向为图像处理等;张 涛(1977—),男,副教授,主要研究方向为信息隐藏等。

会产生较明显的异常。图 1 是大小为 512×512 的标准图像 man. bmp 嵌入率为 100%的 LSB 匹配隐写前后的直方图。

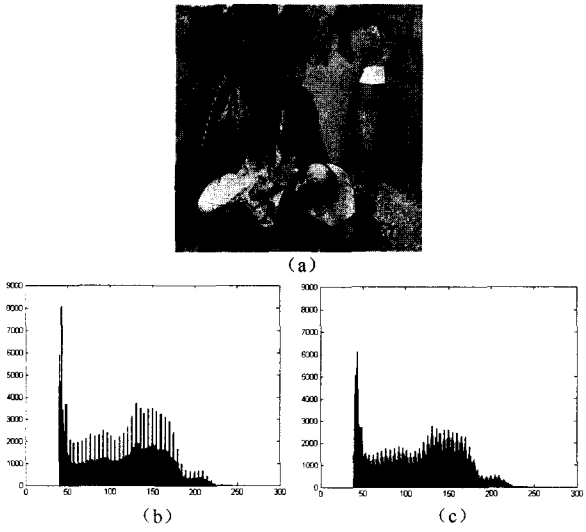


图 1 (a)载体图像 man. bmp,大小 512×512;(b)载体图像灰度直方图;(c) 载密图像灰度直方图

从图 1 可看出,采用 LSB 匹配算法进行隐写后,载密图像和载体图像灰度直方图有明显差异:载密图像的直方图峰值明显减小,整体趋于平缓。LSB 匹配隐写算法产生灰度直方图平滑的原因在于[8]:LSB 匹配隐写对载体图像的每个像素的嵌入修改为:

$$p_s=\begin{cases}p_c+1, & \text{if } b\neq LSB(p_c) \text{ and}(\kappa>0 \text{ or } p_c=0)\\ p_c-1, & \text{if } b\neq LSB(p_c) \text{ and}(\kappa<0 \text{ or } p_c=255)\\ p_c, & \text{if } b=LSB(p_c)\end{cases} \tag{1}$$

式中,$p_c$ 表示载体图像当前像素的灰度值,$p_s$ 是载密图像上相应像素的灰度值;$b\in\{0,1\}$是待隐藏的秘密比特;$\kappa$ 是在$\{-1,1\}$上均匀分布的独立同分布随机变量。通常,秘密信息是通过加密处理的比特流,因此 $b$ 为 0 的概率 $P\{b=0\}$和 $b$ 为 1 的概率 $P\{b=1\}$相同,都为 0.5;而 $\kappa$ 的分布决定了 $P\{\kappa<0\}=P\{\kappa>0\}=0.5$;因此,在不计 $p_c=0$ 和 $p_c=255$ 的条件下,对于嵌入率为 $\rho$ 的 LSB 匹配隐写,有:

$$P\{p_s=p_c\}=P\{b=LSB(p_c)\}\cdot\rho+(1-\rho)=1-\frac{\rho}{2} \tag{2}$$

$$P\{p_s=p_c+1\}=P\{b\neq LSB(p_c)\}\cdot P\{\kappa>0\}\cdot\rho=\frac{\rho}{4} \tag{3}$$

$$P\{p_s=p_c+1\}=P\{b\neq LSB(p_c)\}\cdot P\{\kappa<0\}\cdot\rho=\frac{\rho}{4} \tag{4}$$

因此,嵌入秘密比特后像素灰度值为 $k\in[2,255]$的可能性为:

$$h_s(k)=\frac{\rho}{4}h_c(k-1)+(1-\frac{\rho}{2})h_c(k)+\frac{\rho}{4}h_c(k+1) \tag{5}$$

式中,$h_c(k)$表示载体图像中灰度值为 $k$ 的像素出现的频率,而 $h_s(k)$表示载体图像中灰度值为 $k$ 的像素出现的频率,这样,从直方图来看,采用 LSB 匹配隐写后相当于将载体图像的直方图和模板$\{\frac{\rho}{4},1-\frac{\rho}{2},\frac{\rho}{4}\}$进行卷积,由此造成载密图像直方图的平滑,正是这种平滑作用,给攻击者提供了成功分析的机会。

## 2.2 基于相邻灰度值对互补嵌入的 LSB 匹配隐写改进算法

通过图像像素的最低位面隐藏秘密信息的隐写算法,是依靠修改像素灰度值实现秘密数据的隐藏的。而直方图是对图像灰度值出现频次的统计,因此隐写后的图像直方图的特性必然会受嵌入影响而产生变化。考察 LSB 匹配算法的嵌入修改对直方图的影响:令 $h^{(i)}(k)$表示第 $i$ 次嵌入操作后灰度值 $k$ 的频次,若第 $i$ 次嵌入修改发生在灰度值为 $k$ 的像素 $A(x,y)$上,则嵌入修改除了影响到当前像素 $A(x,y)$的灰度值 $k$ 的出现频次外,还相应改变了相邻灰度值 $k+1$ 或 $k-1$ 的出现频次,即:

$$\begin{cases}h^{(i)}(k)=h^{(i-1)}(k)-1\\ h^{(i)}(k+1)=h^{(i-1)}(k+1)+1 & \text{(当前像素灰度值+1 时)}\\ h^{(i)}(k-1)=h^{(i-1)}(k-1)+1 & \text{(当前像素灰度值−1 时)}\end{cases} \tag{6}$$

未进行嵌入修改时有的图像就是载体图像,因此:

$$h^{(0)}(k)=h_c(k) \tag{7}$$

如果总嵌入修改次数为 $M$,则所有嵌入修改完成后得到的即是载密图像,有:

$$h^{(M)}(k)=h_s(k) \tag{8}$$

式(6)、式(7)和式(8)共同描述了 LSB 匹配隐写对整幅图像的嵌入修改过程。由此可知,嵌入修改对直方图的影响是成对发生的,对一个像素进行嵌入修改,使该像素本身的灰度值频次减少 1,而使与其相邻的灰度值之一的频次增加 1。因此如果在所有需要进行嵌入修改的像素中,能够找到两个像素 $A$ 和 $B$,它们的灰度值相邻,则可以对这两个像素的灰度值进行互补修改,使它们的改变对整个图像的灰度直方图不产生影响。不妨假设像素 $A$ 的灰度值为 $k$,而 $B$ 的灰度值为 $k+1$,第 $i$ 次修改是对像素 $A$ 的灰度值加 1,而第 $i+1$ 次修改是对像素 $B$ 减 1,则第 $i$ 次修改后 $k$ 和 $k+1$ 的出现频次为:

$$\begin{cases}h^{(i)}(k)=h^{(i-1)}(k)-1\\ h^{(i)}(k+1)=h^{(i-1)}(k+1)+1\end{cases} \tag{9}$$

而第 $i+1$ 次修改后 $k$ 和 $k+1$ 的出现的频次为:

$$\begin{cases}h^{(i+1)}(k+1)=h^{(i)}(k+1)-1\\ h^{(i+1)}(k)=h^{(i)}(k)+1\end{cases} \tag{10}$$

那么,这两次嵌入修改对直方图的影响综合为:

$$\begin{cases}h^{(i+1)}(k)=h^{(i-1)}(k)\\ h^{(i+1)}(k+1)=h^{(i-1)}(k+1)\end{cases} \tag{11}$$

即对像素 $A$ 和像素 $B$ 的嵌入修改前后两像素灰度值的出现频次没有任何变化。将满足修改后两像素灰度值频次不变的一对具有相邻灰度值的像素称为匹配像素对,从对相邻灰度值像素 $A$、$B$ 嵌入修改的分析所得的表达式(9)、式(10)和式(11)可以看出,$A$ 和 $B$ 若要构成匹配像素对,则需满足以下两个条件:

①$LSB(p_c(A))\neq b_1$ 且 $LSB(p_c(B))\neq b_2$

②$p_c(A)=p_c(B)+1$ 或 $p_c(A)=p_c(B)-1$

式中,$p_c(A)$和 $p_c(B)$表示载体图像 $A$ 像素和 $B$ 像素的灰度值,$b_1$ 和 $b_2$ 分别是像素 $A$ 和像素 $B$ 要嵌入的秘密比特。条件 1 要求两个匹配像素都是要进行嵌入修改的像素;条件 2 要求像素 $A$ 的灰度值和像素 $B$ 的灰度值是相邻的。同时,对匹配像素的嵌入修改必须是互补的,即对灰度值大的像素进行减 1 嵌入,而对灰度值小的像素进行加 1 嵌入,保证嵌入后

两像素的灰度值互换。

若嵌入修改全部发生在匹配像素对上，则应用该方法能够完全保持直方图特性在嵌入前后不变，但实际上，载体图像中总会有少部分像素无法找到匹配像素，对这些非匹配像素的嵌入修改仍会改变图像直方图特性，因而能找到的匹配像素对越多，直方图特性就保持得越好。载体图像直方图的连续性是保证找到匹配像素的前提。自然图像大多是连续色调图像，因此多数能满足灰度值连续的条件。当以自然图像为载体时，图像中绝大部分像素都可以找到相应的匹配像素，只有少数像素是非匹配的，通过对匹配像素对进行互补嵌入可以大幅减少隐写对直方图特性的改变。

在此基础上，对 LSB 匹配隐写算法进行改进，改进算法的一次嵌入步骤如下：

第一步　判断秘密信息 $b$ 与当前像素 $A$ 的 LSB 是否相等，若相等，则不做修改，将该像素标识为处理过，取下一个像素嵌入；若不相等，则进入第二步；

第二步　从图像未经处理的像素中寻找距离当前像素 $A$ 最近的匹配像素 $B$，如果找到，进入第三步，没有找到，进入第四步；

第三步　对匹配像素 $A$ 和 $B$ 的灰度值进行互补修改，并将像素 $A$、$B$ 标识为处理过；

第四步　对非匹配像素 $A$ 进行随机 $\pm 1$ 嵌入修改，并将像素 $A$ 标识为处理过。

对图像中的所有要嵌入秘密信息的像素进行如上嵌入处理后即可得到载密图像。改进算法的秘密信息仍然隐藏在图像的 LSB 位面，因此，提取方法与 LSB 匹配相同。

### 2.3　改进算法的性能分析

无论是嵌入修改的像素个数还是对单个像素灰度值的修改幅度，改进算法都和 LSB 匹配算法完全相同，因此两者对图像质量的影响是完全相同的，即改进算法保留了 LSB 匹配算法良好的视觉隐蔽性。但不同的是，改进算法利用匹配像素对对直方图修改的互补特性保证了只有少数嵌入修改影响直方图，从而达到保持直方图特性的效果，这一点是 LSB 匹配隐写所无法实现的。

从改进算法的原理可知，对匹配像素对的嵌入修改不改变直方图特性，只有对非匹配像素的修改才改变图像的直方图，因此改进算法对直方图的保持效果取决于非匹配嵌入修改的像素数和嵌入修改总像素数的比值，用参数 $\gamma$ 表示该比值：

$$\gamma=\frac{\text{非匹配嵌入修改像素数}}{\text{嵌入修改的像素数}} \quad \gamma\leqslant 1$$

在该参数定义下，重新考察隐写算法对直方图的影响：

$$\begin{aligned}P\{p_s=p_c+1\}&=P\{b\neq LSB(p_c)\}\cdot P\{\kappa>0\}\cdot\rho\cdot P\{\text{非匹配嵌入}\mid\text{嵌入修改}\}\\&=(P\{b=1\}\cdot P\{LSB(p_c)=0\}+P\{b=0\}\cdot P\{LSB(p_c)=1\})\cdot\rho\gamma\cdot P\{\kappa>0\}=\frac{\rho\gamma}{4}\end{aligned}\tag{12}$$

同理可推：

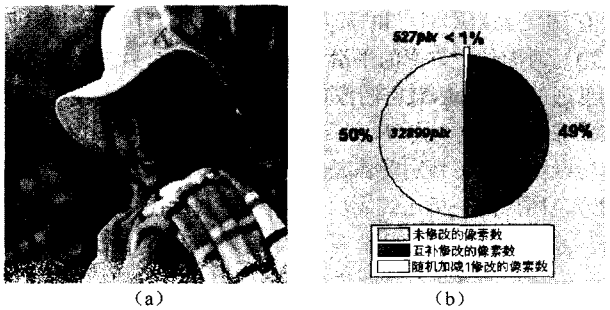
$$P\{p_s=p_c-1\}=\frac{\rho\gamma}{4}\tag{13}$$

$$P\{p_s=p_c\}=1-\frac{\rho\gamma}{2}$$

因此，隐写后载密图像直方图和载体图像直方图的关系满足：

$$h_s(k)=\frac{\rho\gamma}{4}h_c(k-1)+(1-\frac{\rho\gamma}{2})h_c(k)+\frac{\rho\gamma}{4}h_c(k+1)\tag{14}$$

从式(14)可得，只要 $\gamma<1$，利用改进算法得到的载密图像的直方图和原始图像直方图之间的相似程度就高于 LSB 匹配隐写算法。而从 $\gamma$ 的定义来看，$\gamma\leqslant 1$，当且仅当所有需要嵌入修改的像素都是非匹配像素时，当 $\gamma=1$，该算法退化为 LSB 匹配算法。为了更直观地展示 $\gamma$ 取值的大小，图 2(a)在一幅大小为 256×256 的标准图像 elaine. bmp 中用灰度值为 255 的点标识出所有非匹配像素，从被标识的像素比例来看，自然图像载体中的非匹配像素比例非常小。图 2(b)统计了用改进算法对 elaine. bmp 图像进行 100%隐写时，匹配像素对、非匹配像素以及不需修改的像素所占的比例。统计显示，需要进行随机±1 修改的非匹配像素所占比例小于 1%，而满足匹配条件可进行直方图互补修改的像素比例占 49%。统计表明使用改进算法时只有不到 1%的嵌入修改会影响直方图特性，而若使用 LSB 匹配算法进行 100%嵌入，则所有嵌入修改都影响直方图特性，即影响直方图特性的修改为 50%，因此，对于本幅图像，改进方法对直方图的影响仅是 LSB 匹配隐写算法的 2%。这个比例，正是 $\gamma$ 的值。因此，参数 $\gamma$ 不仅表明了改进的隐写算法对直方图的保持能力，而且还是改进算法和原算法的一个定量比较。



(a)　(b)

图 2　(a)256×256 的标准图像 elaine 中非匹配像素显示图；(b)256×256 的标准图像 elaine 中非匹配像素、匹配像素比例

## 3　实验与分析

### 3.1　典型图像的实验结果

以加密后的二进制比特流为秘密信息，分别使用 LSB 匹配和本文提出的改进方案对图 1 所示例图进行 100%的隐写，得到改进算法隐写后的直方图及两种算法隐写前后图像直方图的差，如图 3 所示。

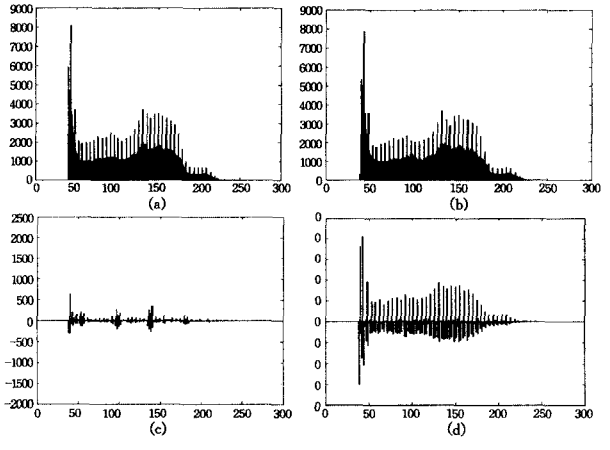



图 3　(a)隐写前载体图像直方图；(b)改进算法 100%隐写后直方图；(c)改进算法隐写前后直方图之差；(d) LSB 匹配隐写前后直方图之差

从图 3(a)(b)可看出，采用改进算法的载密图像并没有出现明显的直方图平滑现象，载密图像与载体图像的直方图非常相似。图 3(c)(d)对比了 LSB 匹配隐写和改进算法载体图像和载密图像直方图的差，表明了新方法在直方图保持上具有很大优势。

参数 $\gamma$ 是定量衡量改进算法性能的一个指标，本文考察了该参数在不同载体图像情况下的取值：表 1 分别统计了 200 幅不同大小的灰度图像的 $\gamma$ 值，从统计结果可得出以下结论：对于一般自然图像，$\gamma \ll 1$ 且随着载体图像尺寸越大，$\gamma$ 值越小；表 1 的统计结果说明，当以自然图像为载体时，改进算法在直方图保持上明显优于传统算法；载体图像尺寸越大，改进算法的优势越明显。

表 1　图像大小对 $\gamma$ 的影响

| | γ_min | γ_max | γ_mean |
|---|---|---|---|
| 128×128 | 0.009569 | 0.258353 | 0.063309 |
| 256×256 | 0.003043 | 0.098913 | 0.013693 |
| 512×512 | 0.002402 | 0.040562 | 0.006325 |

### 3.2　抗直方图分析实验结果

目前基于一维直方图的 LSB 匹配隐写分析基本算法主要有“质心法(COM)”和“局部极值法(ALE)”两种。LSB 匹配隐写对图像直方图的平滑作用从频域来看，就是对直方图的低通滤波，因此，载密图像直方图的高频分量的幅度小于载体图像。利用这一点，Harmsen 提出[3]，通过检测图像直方图特征函数的质心判别图像是否经过 LSB 匹配隐写。该方法对彩色图像的分析比较成功，但是对于灰度图像效果并不显著。基于对 LSB 匹配隐写后的灰度图像的研究，Ker 对 Harmsen 的方法进行了改进[4]，利用下采样后图像的直方图函数对原图直方图函数进行校准，以校准后的参数作为特征进行分析，对灰度图像的分析成功率明显提高。局部极值法是另一种效果较好的针对 LSB 匹配隐写的分析方法，LSB 匹配隐写对图像直方图的平滑使载密图像直方图的局部极大值减小，而局部极小值增大。J. Zhang 等人[5]据此提出了局部极值法检测载密图像。Cox 等人对该方法进行了改进[8]，添加了针对边界值的检测，使这一方法更加完善。

本文分别从文献[9]所述的 Camera 图像库和 NRCS 图像库中随机选取了 1000 幅 BMP 图像，利用 LSB 匹配隐写方法和本文提出的基于相邻灰度值互补嵌入的改进方法进行了嵌入率为 100%的隐写，利用校准的质心法以及考虑边界效应的局部极值法进行了检测。图 4 所示为对两种隐写方法利用不同分析方法得到的 ROC 曲线。

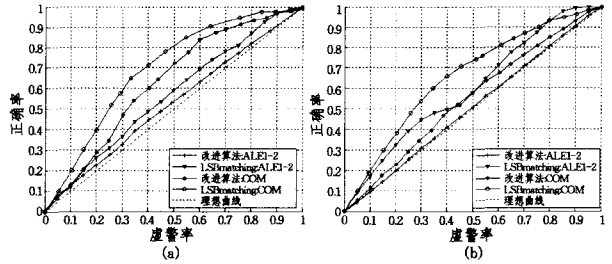



图 4　(a)Camera 图像库的 ROC 曲线；(b)NRCS 图像库的 ROC 曲线(在用局部极值法进行检测时，从样本中随机选取 50%作为训练样本，剩余 50%作为测试样本，取十次平均最为最终结果)

从图中可以看出，无论是用 Camera 图像库还是 NRCS 图像库，无论采用质心法还是局部极值法，在同等虚警率下，改进算法分析的正确率都明显低于传统 LSB 匹配隐写方法。

**结束语**　为了减小 LSB 隐写对直方图分布产生的影响，提高隐写算法的抗分析能力，本文基于对 LSB 匹配隐写方法和利用图像直方图的隐写分析方法的研究，提出了一种基于相邻灰度值互补嵌入的 LSB 匹配隐写改进算法。该算法以灰度值相邻的匹配像素对为对象进行互补嵌入，大幅减少了可能引起直方图改变的嵌入修改的发生。该算法对单个像素灰度值的修改幅度仍为 1，同时最高嵌入率仍为 100%，所以其保留了 LSB 匹配隐写算法视觉隐蔽性好、嵌入率高的优势，但改进算法利用了相邻灰度值像素+1 和−1 操作对直方图影响的互补特性，在直方图保持上具有 LSB 匹配算法所无法达到的效果。

实验表明，本文提出的隐写算法相对于 LSB 匹配隐写方法有了很大的改进，在抵抗各种基于一维直方图攻击上明显优于 LSB 匹配隐写方法。但由于该算法的出发点是一维直方图的保持，因此对目前出现的各种针对二维邻接直方图的攻击其抵御能力并不比 LSB 匹配隐写方法更具优势，所以需要深入研究 LSB 匹配隐写图像邻接直方图特性，以考虑二维直方图保持的隐写算法。

## 参 考 文 献


[1] Westfeld A, Tzmann A P. Attacks on steganographic systems [C]// 3 Inlernalional Workshop 011 Inybrmation Hiding. 1999

[2] Fridrich J, Goljan M, Du R. Detecting lsb steganography in color and gray scale images[C]// IEEE Multime—dia Special Issue on SP c'urity. 2001: 22-23

[3] Harmsen J, Pearlman W. Steganalysis of additive noise modelable information hiding in Security and Watermarking of Multimedia Contents V[C]//Proceedings of SPIE. vol. 5020, January 2003: 131-142

[4] Andrew D. Ker Steganalysis of LSB Matching in Grayscale Images[J]. IEEE Signal Processing Letters, 2005, 16(6): 441-444

[5] Zhang J, Cox I J, Döerr G. Steganalysis for LSB matching in images with high-frequency noise[C]// Proceedings of the IEEE Workshop on Multimedia Signal Processing. October 2007: 385-388

[6] 赵鸿冰，林代茂，杨怀江. 利用反馈控制直方图失真的隐写方法[J]. 光学精密工程，2006，14(4)：720-724

[7] 陈志宏，刘文耀. 保持直方图特性的最低比特位密写方法[J]. 天津大学学报，2008，41(1)：21-27

[8] Cancelli G, Döerr G, Cox I J, et al. Detection of ±1 Lsb Steganography Based on the Amplitude of Histogram Local Extrema [C]// International Conference on Image Processing. 2008: 1288-1291

[9] Cancelli G, Döerr G, Barni M, et al. Cox A Comparative Study of ±1 Steganalyzers [C]// Proceedings of the IEEE International Workshop on Multimedia Signal Processing. 2008: 791-796