文章编号 1004-924X(2006)04-0001-04

利用反馈控制直方图失真的隐写方法

赵鸿冰,林代茂,杨怀江
(1. 中国科学院 长春光学精密机械与物理研究所,吉林 长春 130033;
2. 北京电子技术应用研究所,北京 100091)

摘要:直方图是图像最重要的特征量,经常被攻击者作为分析的凭证,设法使隐写后的直方图失真尽量小是抵御直方图攻击的有效手段。本文通过对±嵌入隐写产生的直方图失真进行分析,提出利用直方图失真反馈对嵌入进行调整的新思路,并结合该思路对±1 嵌入隐写方法进行了改进。实验结果表明,通过该方法,直方图的实际失真达到了理论的最小值,从而提高了隐写的安全性。而本文仅是将该方法应用到时域的嵌入方法中,也可以将该方法应用于频域的嵌入方法。

关 键 词:隐写术;直方图最小失真;最小方差隐写;最小相对隐写
中图分类号:TH703 **文献标识码**:A

Steganography with controlling histogram abnormality using feedback

ZHAO Hong-bing, LIN Dai-mao, YANG Huai-jiang

(1. *Changchun Institute of Optics, Fine Machanics and Physics, Chinese Academy of Sciences, Changchun*, 130033, *china*; 2. *Beijing Institute of Electronic Technology and Application, Beijing*, 100091, *China*)

Abstract: The histogram of an image is a key feature statistic, which is often searched by attackers for artifact caused by steganography. Therefore, keeping the abnormality of histogram minimum can be an efficient way to resist steganalysis based on histogram. In this paper, we first analyze the abnormality of histogram caused by ±1 embedding, and present a new idea of regulating the process of embedding by the feedback of the abnormality of histogram. Based on this new idea, we have improved the ±1 embedding method. Experimental results show that using the method advanced here, the practical abnormality of histogram is theoretically minimum, and the security of steganography is consequently improved. Though we only apply the method in time-domain embedding in this paper, we think it is also promising in frequency-domain.

Key words: steganography; least histogram abnormality; least variance embedding; least relative embedding

收稿日期:2005-11-18;**修订日期**:2006-08-11.
基金项目:国家 973 计划资助项目(No. TG1999035804)

1 引　言

隐写术是信息隐藏技术的一个重要分支，主要应用于隐蔽通信。与信息隐藏技术的另一主要分支—数字水印相比，由于应用背景的不同，对其三项基本特性的要求重点也不同。隐写术最注重隐蔽性即不能让攻击者有证据地怀疑密信的存在；通信的目的即要传递一定的信息，嵌入量是隐写术其次关注的；而隐写术一般不把防御主动攻击作为重点，故鲁棒性为最后所关注。LSB 隐写技术是最早出现的隐写术，其实现简单、隐藏数据量大，至今还得到广泛的关注。

LSB 隐写是用像素灰度的最低比特位来代表秘密信息(也有人用频域系数的最低比特位替换，本文不讨论)，其变换部分实质是 $x_{2j}\leftrightarrow x_{2j+1}$ (其中 x_{2j} 代表灰度值为 $2j$ 的像素)。然而这种变换是非对称的，它将产生对称的直方图失真，而由再次进行的对称变换又会产生非对称的现象，这些都可以被攻击者作为成功分析的依据。

χ^2 分析[1]和 RS 分析[2]是针对 LSB 的两种经典的隐写分析方法。从直方图的角度看，LSB 引起 $h_{2j}\leftrightarrow h_{2j+1}$ (其中 h 代表直方图，h_{2j} 代表灰度值为 $2j$ 的像素总数)的变化。为保证密信的安全性，在嵌入之前通常要对密信进行加密，从而嵌入的密信就变成了随机分布的、出现概率对等的 0，1 比特流。这样，如果对图像进行满嵌，那么 h_{2j} 与 h_{2j+1} 就会近似相等，出现所谓的 Pairs of Values (PoV's)，χ^2 分析利用这一现象对 LSB 实施了有效的攻击。RS 分析定义 $x_{2j}\leftrightarrow x_{2j+1}$ 为正翻转，$x_{2j}\leftrightarrow x_{2j-1}$ 为负翻转，发现经过 LSB 隐写的图像会对再次的正负翻转呈现出非对称的变化，据此对 LSB 实施了有效的攻击。

针对 LSB 的有效的攻击方法的出现推动了研究者对其进行改进。$+-1$ 嵌入方法[3]在隐写时主动加入负翻转，使得正负翻转达到对称，这样前面提到的统计攻击特性就不复存在了。加入负翻转虽然已影响到倒数第二个比特位，但从像素改变的最大幅度看，仍旧是 1，像素间的相关性并未受到过大的破坏；而从人类视觉系统(HVS)的角度来讲，这种改变是人眼所不能分辨的。$+-1$ 嵌入方法虽然调整了对称性，但没有顾及直方图的变化，这给直方图形成新的攻击特征留下了隐患。文献[4]将一些隐写(包括 $+-1$ 嵌入)过程建模成对图像直方图低通滤波的过程，这样利用图像直方图频谱(高频部分)的变化实现了隐写分析。

如果隐写方法能使直方图失真最小，就可以抵御上述分析方法的攻击。本文提出的隐写方法就是建立在直方图失真最小化的基础上。

2 直方图最小失真隐写

2.1 直方图最小失真定义

设隐写后直方图的失真为 d_j，$d_j\in R$，

$$d_j=h_j'-h_j\ (0\leqslant j\leqslant 255)\ , \tag{1}$$

其中 h_j 代表原图灰度为 j 的像素总数，h_j' 代表隐写后图像中灰度为 j 的像素总数。则

最小线性失真定义为：

$$A_{\min}=Min\Big(\sum_{j=0}^{255}|d_j|\Big)\ , \tag{2}$$

最小方差失真定义为：

$$V_{\min}=Min\Big(\sum_{j=0}^{255}d_j^2\Big)\ , \tag{3}$$

最小相对失真定义为：

$$R_{\min}=Min\Big(\sum_{j=0}^{255}\Big|\frac{d_j}{h_j}\Big|\Big)\ , \tag{4}$$

不难看出后两种定义是以最小线性失真为基础的。

2.2 $+-1$ 嵌入方法直方图失真规避

图 1 为 $+-1$ 嵌入方法直方图变化示意图。用 $\overleftrightarrow{h_j}$ 表示由 x_j 向 x_{j-1} 和 x_{j+1} 翻出的总数，$\overrightarrow{h_{j-1}}$ 和 $\overleftarrow{h_{j+1}}$ 分别表示由 x_{j-1} 和 x_{j+1} 向 x_j 翻入的总数，则直方图失真 d_j 可以表达为：

$$d_j=(\overrightarrow{h_{j-1}}+\overleftarrow{h_{j+1}})-\overleftrightarrow{h_j}\ , \tag{5}$$

由于 0 与 255 分别只能作正与负翻转，所以规定 $\overrightarrow{h_{-1}}=0$，$\overleftarrow{h_{256}}=0$ 。

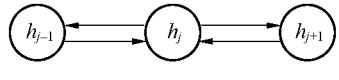


图 1　$+-1$ 嵌入方法直方图变化示意图

Fig. 1

我们的目的是使 d_j 满足式(3)或者式(4)。首先需要使 d_j 满足式(2)，即使 $|d_j|\to 0$。从式(5)中可以看出，d_j 决定于 $(\overrightarrow{h_{j-1}}+\overleftarrow{h_{j+1}})$ 与 $\overleftrightarrow{h_j}$ 的

差，而对给定的载体与密信，$\overleftrightarrow{h_j}$ 是确定的，d_j 只决定于 $(h_{j-1}+\overleftarrow{h_{j+1}})$。改变 $(\overrightarrow{h_{j-1}}+\overleftarrow{h_{j+1}})$ 使 $d_j \to 0$。

当 $j=0$ 时，$d_0=\overleftarrow{h_1}-\overleftrightarrow{h_0}$，若使 $d_0=0$，由于 $\overleftrightarrow{h_0}$ 不可变，作调整 $\overleftarrow{h_1}=\overleftarrow{h_1}-d_0$，其实际意义是将原来 h_1 向 h_0 翻转的数目减掉 d_0 个，为保证 $\overleftrightarrow{h_1}$ 不变，使 $\overrightarrow{h_1}=\overrightarrow{h_1}+d_0$，其实际意义是将 h_1 向 h_2 翻转的数目增加 d_0 个，显然这影响到 d_2，将这个影响同步加到 d_2，即 $d_2=d_2+d_0$。当 $j=1$ 时，$d_1=(\overrightarrow{h_0}+\overleftarrow{h_2})-\overleftrightarrow{h_1}$，若使 $d_1=0$，$\overleftrightarrow{h_1}$ 不可变，$\overrightarrow{h_0}$ 已由前面的调整固定，这样只能作调整 $\overleftarrow{h_2}=\overleftarrow{h_2}-d_1$，同步使 $\overrightarrow{h_2}=\overrightarrow{h_2}+d_1$，受到影响的 d_3 也作更改，$d_3=d_3+d_1$。同理依此类推，

$$\overleftarrow{h_j}=\overleftarrow{h_j}-d_{j-1},\overrightarrow{h_j}=\overrightarrow{h_j}+d_{j-1},d_{j+1}=d_{j+1}+d_{j-1}, \tag{6}$$

在满足下述两个条件的特殊情况下，经过(6)的调整能使所有的 d_j 都等于 0，而使得直方图无损：(1)保证载体直方图较平滑。符合此条件能满足 $\overleftarrow{h_j}$ 大于 d_{j-1}，使调整的结果不留下局部失真。(2) 奇像素(灰度值为奇数的像素)向偶像素(灰度值为偶数的像素)翻转的总数等于偶像素向奇像素翻转的总数。正负翻转实质上是像素灰度值奇偶转化的过程，而如果隐写前后奇偶数量有了差异，直方图一定有损。而这一条件取决于载体与密信的耦合特性，这样的概率相当小。

用 O_a 代表奇像素失真、E_a 代表偶像素失真，由于正负翻转是像素灰度值奇偶转化的过程，所以 $O_a=-E_a$，理论上，$A_{\min}=2|O_a|=2|E_a|$，在满足条件 1)的情况下，通过式(6)的调整会使直方图失真达到这个最小的理论值。经过式(6)的调整，使绝大多数 d_j 等于 0，也使最小线性失真积累到最后。而将这个失真积累到载体直方图的一端时，一般载体的直方图端部都不能满足 $\overleftarrow{h_j}$ 大于 d_{j-1}，所以我们采取的是从两端向峰值调整，这样使得最小线性失真积累到峰值处。从右端向左调整的表达式的推导过程与式(6)的推导过程类似。至此，我们已经使得隐写后直方图达到最小线性失真。

然而，我们将最小线性失真积累到峰值处，这似乎是帮助破坏者积累了攻击特征，必须考虑把最小线性失真分散到直方图的各个部分中去。

在式(6)的调整中，使 $d_j=0$，才使得最小线性失真向某一处积累。如果在这步调整中，按照某种分散策略，将各个失真留在相应的 d_j 就可以将最小线性失真分散到直方图的各个部分，即将式(6)变为

$$\overleftarrow{h_j}=\overleftarrow{h_j}+d_{j-1}-a_j,\overrightarrow{h_j}=\overrightarrow{h_j}-d_{j-1}+a_j,d_{j+1}=d_{j+1}-d_{j-1}+a_j \tag{7}$$

其中 a_j 为分散部分。

按照不同的要求，对应不同的分散策略，a_j 取值定义也不同。如果要求直方图达到最小方差失真，即满足(3)，那么须将最小线性失真 $A_{\min}$ 均匀的分布到直方图中，此时，$a_j=A_{\min}/\mathrm{sum}$，其中 sum 为直方图中大于某一域值的灰度个数；如果要求直方图达到最小相对失真，即满足(4)，此时，$a_j=A_{\min}\times(h_j/H)$，其中 $H=\sum_{j=0}^{255}h_j$；也可以将 $A_{\min}$ 随机的分散到直方图中。

2.3　嵌入步骤

本算法仍采用 ±1 嵌入方式，但是利用直方图失真反馈来调整像素的正负翻转，使得直方图达到最小失真。具体步骤描述如下：

1) 首先进行 ±1 预嵌入，即在保证正负翻转总数相等的前提下，对照密信，将需要改变的像素进行随机的正负翻转，统计直方图失真 d_j，统计奇偶翻转最小线性失真 $A_{\min}$，分别计算满足式(3)、式(4)条件下的 a_j。

2) 计算调整量 $\overleftarrow{h_j}$、$\overrightarrow{h_j}$。

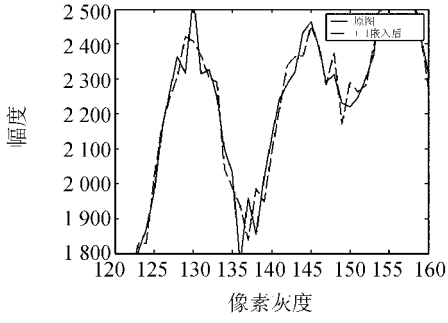
3) 结合调整量进行正式嵌入。

需要强调的是，在整个过程中正负翻转总数总是相等的，不会给现有的利用正负翻转不对称的攻击方法留有任何的机会。

3　实验结果与分析

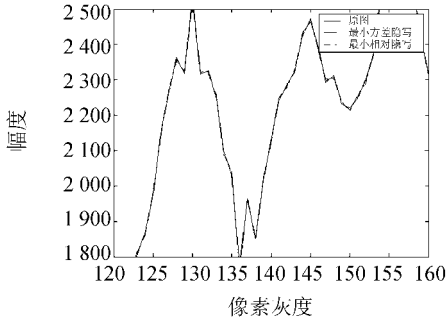
以大小为 512×512 的灰度 lena 为测试图，使每个像素都携带 1 比特的信息，分别做 ±1 嵌入隐写、最小方差隐写(直方图最小方差失真隐写)和最小相对隐写(直方图最小相对失真隐写)。图 2 给出了原图直方图与三种隐写后图像直方图的局部对比。

图 2(a)显示 ±1 嵌入隐写后图像直方图有明显的失真，而从图 2(b)中可看出，经过最小方差隐写和最小相对隐写后图像直方图与原图直方图几乎看不出差别。为更清晰刻划三种隐写对图



(a)原图直方图与±1 嵌入隐写后图像直方图局部对比

(a)



(b) 原图直方图与最小方差隐写和最小对隐写后图像直方图局部对比

(b)

图 2

Fig. 2

像直方图造成的失真，将各隐写导致的失真绘于图 3。通过图 3(a)与图 3(b)的对比可看出，最小方差隐写和最小相对隐写比±1 嵌入隐写导致的直方图失真绝大多数都小一个量级。

直方图失真幅度小能很好地保持其频谱的特征。图 4 绘出了三种隐写导致的图像直方图频谱

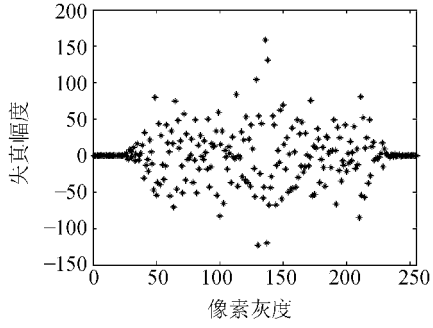
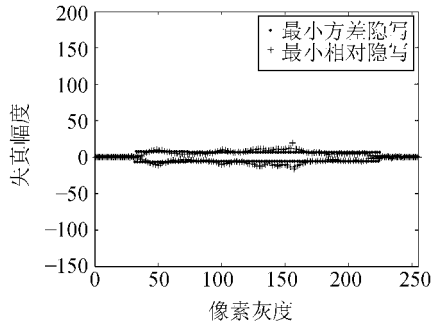


图 3(a)±1 嵌入隐写导致图像直方图失真

(a)



(b) 最小方差隐写和最小相对隐写导致图像直方图失真

(b)

图 3

Fig. 3

高频部分的失真。从图 4(a)与(b)的对比可看出，最小方差隐写和最小相对隐写很好的保持了直方图的频谱特征，从而可有效地抵抗利用直方图频谱作分析依据的攻击。

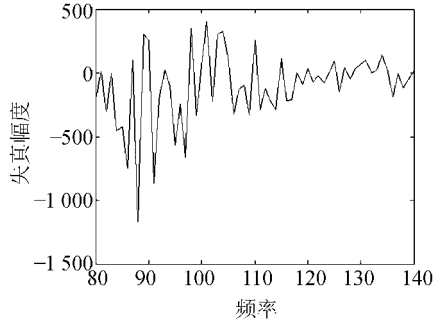
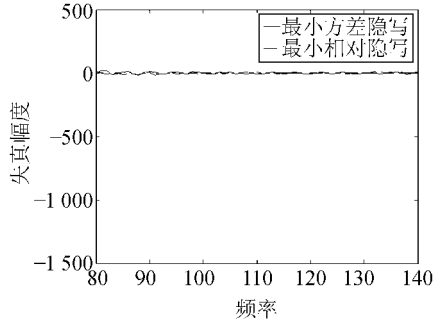


图 4(a)±1 嵌入隐写导致图像直方图频谱失真

(a)



(b) 最小方差隐写和最小相对隐写导致图像直方图频谱失真

(b)

图 4

Fig. 4

4 结　论

本文提出了一种新的直方图失真控制隐写思路，可抵抗各种基于直方图的攻击，提高了隐写的安全性。最小方差隐写是将最小线性失真均匀分布到直方图中，最小相对隐写是将最小线性失真按载体直方图的分布而分布到直方图中。实验数据表明，改进方法直方图失真幅度明显小于原方法，从而很好地保持了直方图原来的某些特征，如频谱特征。两种方法都是在保证直方图达到最小线性失真的前提下，消除直方图失真特征，从而使分析者的攻击更具难度。

为取得更好的效果，应注意：1）选择直方图较平滑的载体，否则会使局部失真增大。2）. 选择载体使其与密信尽量匹配，即使奇、偶像素失真尽量小，使得最小线性失真越小越好。

另外，可将本方法移植到频域嵌入方法中，能使频域系数直方图的失真得到控制，而使其原有的特征得以保持。

参考文献：

[1] PETITCOLAS F A P，ANDERSON R J，KUHN M G. Information hiding-a survey[C]. *Proceedings of the IEEE, special issue on protection of multimedia content*, 1999，67(7)：1062-1076.

[2] HSU C T，WU J L. Hidden Digital Watermarks In Images[C]. *IEEE Trans. On Image Processing*, 1999，8：58-68.

[3] WESTFELD A. F5－A steganographic algorithm. in 4th international workshop on information hiding[J]. *Lecture Notes in Computer Science*, Spring-Verlag, 2001，2137：289-302.

[4] WESTFELD A，TZMANN A P. Attacks on steganographic systems 3rdInternational Workshop on Information Hiding. 1999.

[5] FRIDRICH J，GOLJAN M，DU R. Detecting lsb steganography in color and gray-scale images[C]. *IEEE Multimedia Special Issue on Security*，2001，22-23.

[6] 隋永新，杨英慧，杨怀江，曹健林. 基于噪声抽取的信息隐藏方法研究光学. 光学精密工程. 2002 年 03 期

[7] 任智斌，隋永新，杨英慧，杨怀江. 以图像为载体的最大意义位(MSB)信息隐藏技术的研究. 光学精密工程. 2002 年 10 卷第 2 期

[9] SHARP T. An implementation of key-based digital signal steganography. In：I. S. Moskowitz (eds.)：4th International Workshop on Information Hiding[J]. *LNCS* 2137, *Springer-Verlag*, *New York*, 2001：13-26.

[9] HARMSEN J J，PEARLMAN W A. Steganalysis of additive noise modelable information hiding[J]. *in Delp III and Wong*，20：131-142.

[10] 王朔中，张新鹏，张开文. 数字密写与密写分析. 北京：清华大学出版社，2005，4

[11] Joyce Van de Vegte 著，候正信，王安国等译. 数字信号处理基础. 北京：电子工业出版社，2004，8

[12] 李忠范，高文森. 数理统计与随机过程. 长春：吉林大学出版社，2000，10.

作者简介：赵鸿冰(1980－)，男，博士生。主要研究信息安全。E-mail：hbing2399@hotmail.com

林代茂(1945－)，男，研究员，博士生导师。主要研究信息安全。

杨怀江(1966－)，男，研究员，博士生导师。主要研究信息安全，光学信息融合。