

针对二值图像信息隐藏的攻击方法^{*}

郭云彪^{1,2}, 胡 岚², 尤新刚^{1,2}, 张春田¹

(1. 天津大学电子信息工程学院, 天津 300072;

2. 北京电子技术应用研究所, 北京 100091)

摘 要: 提出了一种针对二值图像信息隐藏的攻击方法。该方法利用图像滤波理论, 对携带信息的载体图像滤波来预测原始载体图像, 通过计算游程统计规律来检测基于修改游程的信息嵌入。该算法不但可以可靠地判定载体图像是否含有隐藏信息, 而且还能较为准确地估计出嵌入容量。

关键词: 隐秘分析; 攻击; 信息隐藏; 二值图像; 图像处理

中图分类号: TP391.41 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0176-04

二值图像也叫黑白图像, 图像内容只用黑白两个色调表示, 主观视觉对修改黑白像素较为敏感, 因此在黑白图像上进行信息隐藏就更具挑战性。国际上有不少学者针对二值图像信息隐藏进行了诸多探索, 设计出一些可行的信息隐藏算法^[1-7], 但相对于其它格式的数字图像信息隐藏研究而言, 其研究成果还较少, 研究投入也相对薄弱。随着信息隐藏技术研究的不断深入, 与之相对抗的信息隐藏分析研究也开始逐渐流行。然而, 从我们掌握的文献来看, 针对二值图像信息隐藏的分析研究现在还不多见。本文提出了一种图像隐藏分析方法用于检测二值图像信息隐藏, 该方法针对修改游程的隐藏算法, 不但可以可靠地检测二值图像是否含有嵌入信息, 还可以估计嵌入信息的长度。

1 二值图像的信息隐藏方法——游程修改法

日本学者 Matsui 等^[2]提出了一种修改像素游程的信息嵌入方法, 该方法主要针对传真文件实施。传真文件每行包含 1728 个像素, 这 1728 个像素包含有许多游程, 游程数据采用霍夫曼编码记录数据。Matsui 等提出的具体嵌入策略非常简单, 采用修改游程边缘的像素, 使游程加 1 或减 1, 最终用游程的奇偶性来携带信息。尽管文献 [2] 中讨论的图像载体只涉及传真文件, 实际上该嵌入算法可以推广到所有的二值图像。嵌入前后的视觉效果如图 1 所示。

二值图像一般用来表示图文信息, 对于文字内

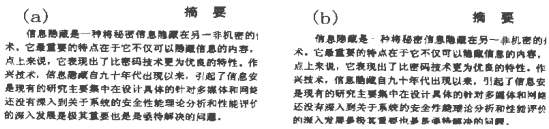


图 1 游程法信息嵌入前后图像比较 (游程加 1 策略)

Fig. 1 The embedding visual effect

(a) 原始图像; (b) 嵌入信息后的图像

容的图像而言, 文字的字型是固定的, 利用游程修改法进行信息嵌入虽然不影响文字的可懂性, 但是可以察觉出文字的视觉变化。从图 2 可以看出, 文字图像经隐藏处理后, 文字的笔画不如原图光滑, 竖笔中有明显的凸凹破缺。因而视觉攻击不失为针对二值图像的一种检测手段。



图 2 游程法信息嵌入前后放大比较 (游程加 1 策略)

Fig. 2 Zoomed embedding visual effect

(a) 原始图像; (b) 嵌入信息后的图像

然而视觉攻击不能从根本上完成二值图像的信息隐藏检测, 图像来源对文字笔画的完美程度有很大的影响。录入文字形成图像其外型取决与字库点阵图像, 通过外设采集的图像其外型取决于图像摄取设备的特性, 同一幅图像同一摄取设备多次采集的图像, 其图像内容并不完全相同, 其字符笔型也存在凸凹破缺 (图 2a), 仅仅靠视觉观察, 并不容

* 收稿日期: 2004-09-11

基金项目: 国家 863 计划资助项目 (2002AA145010); 国家 973 计划资助项目 (TG1999035804)

作者简介: 郭云彪 (1969 年生), 男, 副研究员; E-mail: gybgnx@hotmail.com

易判断这些凸凹破缺是信息嵌入造成的还是图像采集过程形成的。

2 游程统计规律研究方法

本文讨论的二值图像信息隐藏算法的关键就是改变图像的“0”、“1”游程，因此针对该算法检测研究也要从考虑二值图像游程的统计特性入手，找出图像游程的统计规律随信息嵌入的变化情况。

在考察不同游长序列出现概率时，可以用两种方法进行计算：

(1) 对于一个序列，首先对不同游长的 0 序列和 1 序列分别计数，然后求出不同游长在所有游长中所占的百分比。即：

$$n \text{ 游长所占的百分比} = \frac{n \text{ 游长的个数}}{\text{所有游长的总数}} \tag{1}$$

(2) 对于一个序列，首先对不同游长的 0 序列和 1 序列分别计数，用游长数与游长长度相乘，求出该游长在该序列的总位数，用该游长的总位数与序列长度相比即可求出属于不同游长的数据位在该序列所占的百分比。即：

$$n \text{ 游长数据位在该序列百分比} = \frac{n \text{ 游长的个数} \times n}{\text{序列长度}} \tag{2}$$

对于任一个序列，由于其序列长度是固定的，而该序列所有游长的总数具有一定的随机性，因此在研究游长统计规律时第二种方法更为方便实用。本文中我们采用的即是第二种研究方法。

3 信息隐藏算法对游程统计规律的影响

确定了游程统计规律的研究方法，则需考虑利用修改游程进行信息嵌入对游程统计规律的影响。设嵌入前游程 i 出现的概率为 P_i ，嵌入后游程 i 的出现概率为 Q_i ，密文出现“0”的概率为 S_0 ，出现“1”的概率为 S_1 ，则嵌入前后概率转移如图 3 所示：

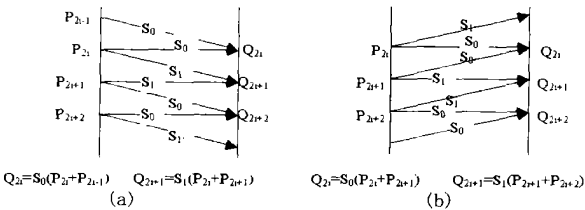


图 3 嵌入前后概率转移图

Fig 3 The embedding model

(a) 游程加 1 策略；(b) 游程减 1 策略

一般在信息嵌入之前，均对要携带的内容进行压缩加密预处理，经预处理后的内容可以看成

伪随机序列，“1”和“0”是等概率出现的，所以 $S_0 = S_1 = 1/2$ ，则

对于游程加 1 策略，则有：

$$Q_{2i} = 1/2(P_{2i} + P_{2i+1}) \dots\dots$$
$$Q_{2i+1} = 1/2(P_{2i} + P_{2i+1}) \tag{3}$$

$$Q_i = 1/2(P_i + P_{i+1}) \tag{4}$$

对于游程减 1 策略，则有：

$$Q_{2i} = 1/2(P_{2i} + P_{2i+1})$$
$$Q_{2i+1} = 1/2(P_{2i+1} + P_{2i+2}) \tag{5}$$

$$Q_i = 1/2(P_i + P_{i+1}) \tag{6}$$

这样看来，信息嵌入处理后图像的游程分布相当于对嵌入前图像游程分布做二阶均值前向或后向平滑（图 4）。

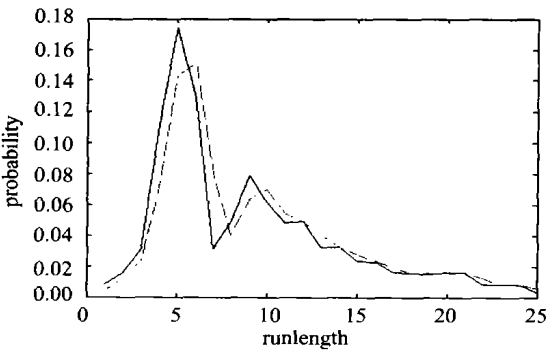


图 4 信息隐藏前后游程统计规律的比较（游程加 1 策略）

Fig 4 The run length distribution of the original and stego image

实线为原始图像游程统计规律曲线，虚线为嵌入信息后游程统计规律曲线

4 利用低通滤波对原始图像的统计特性进行预测

均值平滑处理前后，二值图像的游程统计规律变化不大，从被动攻击的角度而言，我们无法从均值平滑后的概率分布去推测原始二值图像的概率分布，所以还需要设法预测信息隐藏前原始图像的游程分布情况（图 5）。

摘要摘要摘要摘要

图 5 含密滤波后图像、原始图像与嵌入信息后图像之间的比较

Fig 5 The estimation visual effect

(a) 含密滤波后图像；(b) 扫描原始图像；(c) 嵌入信息后的图像

从前面视觉效果图可以看出, 修改游程信息嵌入方法破坏了图像单元的连通性与边界光滑性, 使图像笔画上产生了凸凹破缺, 相当于给图像加入了高频噪声, 利用低通滤波器对载体图像进行低通滤波, 正好可以滤掉这些高频噪声, 去掉图像笔画上的凸凹毛刺, 这样就可以把图像恢复到接近信息隐藏前的情形 (如图 6 所示)。

修改游程法信息嵌入过程可以等效为一个高频噪声加入过程。对于引入噪声的信息隐藏算法, 可以通过低通滤波, 将嵌入引入的高频噪声滤掉, 来估计原始图像。因此就可以用滤波后图像游程的统计特性做原始图像游程统计特性的近似 (如图 7 所示), 通过比较信息隐藏前后游程统计特性的区别来对图像是否进行过信息隐藏做出判断。

滤波器的选择会明显影响滤波后图像对原图的逼近效果, 考虑到嵌入策略为加 1 或减 1, 因此引入的噪声为单像素噪声颗粒。滤波器结构不易过于复杂, 经多次实验选择 3X3 滤波器滤波效果与原图最为逼近。具体滤波器结构如下:

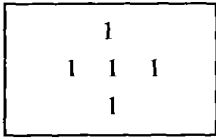


图 6 本技术采用的低通滤波器
Fig. 6 The filter structure

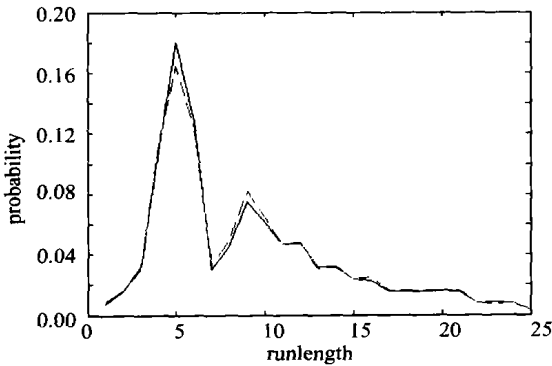


图 7 滤波后信息隐藏前后游程统计规律的比较 (游程加 1 策略)
Fig. 7 The run length distribution of the original and estimated image
实线为原始图像的游程统计规律曲线, 虚线为均值滤波后游程的统计规律曲线

5 嵌入长度的估计

当我们拿到一幅图像后, 我们首先用低通滤波来估计原始图像的游程统计规律, 然后根据公式 8, 用估计得到的原始图像的游程统计规律, 来计

嵌入概率。假设占百分比 β 的长度为 i 游程参与了信息嵌入, 参与信息嵌入的那部分游程的统计规律按公式 (6) 变化, 没有参与信息嵌入的那部分游程统计规律保持不变, 因此只修改 β 游程其嵌入前后统计规律的变化情况可用公式 (7)、(8) 表示。

对于游程加 1 策略

$$Q_i = (1 - \beta) P_i + \beta (P_i + P_{i+1}) \tag{7}$$

对于游程减 1 策略

$$Q_i = (1 - \beta) P_i + \beta (P_i + P_{i-1}) \tag{8}$$

则 $\beta = \frac{2(Q_i - P_i)}{P_{i+1} - P_i}$

或 $\beta = \frac{2(Q_i - P_i)}{P_{i-1} - P_i}$

$$\beta = \arg \min_{\beta} \left\{ \sum_i Q_i - 1(1 - \beta) P_i + \frac{1}{2} \beta (P_i + P_{i+1}) \right\} \tag{9}$$

6 实验结果

本算法采集 50 幅图像作为实验样本, 这些实验样本的图像内容均为文字, 这些文字经图像处理软件直接录入获得, 分辨率从 512×512 到 1728×1024 , 利用前面提到的游程加 1 嵌入策略, 分别以嵌入量为 1%、5%、10% 进行信息嵌入, 然后利用公式 (9) 进行嵌入长度估计, 实验结果如图 8 所示, 从实验结果可以看出估计结果与实际嵌入量非常接近。

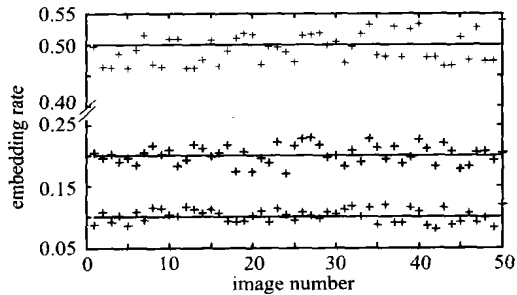


图 8 检测实验结果
Fig. 8 The experimental result

前面已经提到, 图像在摄取过程中, 由于存在量化误差难免会引入高频噪声, 在视觉上也会产生笔画的凸凹破缺, 低通滤波也会有效地消除这些高频噪声, 消除笔画的凸凹毛刺, 使笔画变平滑。因而一幅图像即使不进行信息嵌入处理, 低通滤波处理前后, 其游程统计特性仍可能有微小差别, 特别是当量化噪声较大时, 一幅图像即使没有嵌入信息, 在对原始图像做嵌入长度估计时会存在一定的较大

的原始估计偏差。当然在嵌入量不大时(嵌入引入的高频噪声和图像采集引入的高频噪声有一定可比性时)时检测灵敏度会降低。

参考文献:

[1] . CHEN Y Y, PAN H K, TSENG Y C. A secure data hiding scheme for two-color images [J] . IEEE Transactions on communications, 2002, 50(8) .

[2] TANAKA K, MATSUI K. Video-steganography: how to secretly embed a signature in a picture' [J] . Proc IMA Intellectual Property Project, 1994, 1(1): 187— 205.

[3] PAN H K, CHEN Y Y, TSENG Y C. A secure data hiding scheme for two-color images [C] . IEEE Symposium on Computers and Communications, 2000.

[4] TSENG Y, PAN H. Secure and invisible data hiding in 2— color images [C] . IEEE Symposium on Computers and

Communications, 2000.

[5] WU M, TANG E, LIU B. Data hiding in digital binary images [C] . Proc IEEE Int' l Conf. on Multimedia and Expo, New York, NY. 2000.

[6] KOCH E, ZHAO J. Embedding robust labels into images for copyright protection [C] . Proc International Congress on Intellectual Property Rights for Specialized Information, Knowledge & New Technologies, Vienna, 1995.

[7] MEI Q, WONG E K, MEMON N. Data hiding in binary text documents [C] . SPIE Proc Security and Watermarking of Multimedia Contents III, San Jose, CA. 2001.

[8] 胡岗. 信息隐藏分析与攻击 //第四届全国信息隐藏会议论文集 [C] . 大连, 2002.

[9] 尤新刚. 图像信息隐藏数据特性的研究 //第二届全国信息隐藏会议论文集 [C] . 北京, 2000.

[10] 盛骤. 概率论与数理统计 [M] . 北京: 高等教育出版社, 2000.

Attack on Binary Image Information Hiding

GUO Yun biao^{1,2}, HU Lan², YOU Xin gang^{1,2}, ZHANG Chun tian¹

(1. School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China;
2. Beijing Institute of Electronic Technology and Application, Beijing 100091, China)

Abstract: Many steganalytic techniques of color images were presented in recent years, but only a few of them can be directly applied in binary images. This paper presents a novel steganalytic scheme that can reliably detect messages hidden in binary image using run length modification method. The key element of this scheme is estimation of the original image, which is done by filtering the stego image with low pass filter. This method is able to detect embedding rates.

Key words: steganalysis; attack; information hiding; binary image; image processing