第37卷 第14期 计 算 机 工 程 2011年7月
Vol.37 No.14 Computer Engineering July 2011

·安全技术· 文章编号：1000—3428(2011)14—0125—03 文献标识码：A 中图分类号：TP391

基于像素差和模函数的隐写方法

李 军[1]，潘 峰[1,2]，李秀广[1,3]

(1. 武警工程学院电子技术系网络与信息安全武警部队重点实验室，西安 710086；
2. 西安电子科技大学网络信息安全教育部重点实验室，西安 710071；3. 武警工程学院信息安全研究所，西安 710086)

摘 要：传统的利用像素差(PVD)进行隐写的方法，通常只考虑水平方向的 PVD 而忽略垂直方向的 PVD。为此，将原始图像分成互不相交的 2×2 的像素块，在水平和垂直 2 个方向上分别采用基于模函数的方法和普通 PVD 的方法进行隐写，并针对 2 种方法的特点对越界情况进行调整。实验结果表明，该方案能改善隐写图像的质量，提高嵌入容量，并能抵抗常见攻击。

关键词：像素差；隐写；模函数；嵌入容量

Steganography Method Based on PVD and Modulus Function

LI Jun[1], PAN Feng[1,2], LI Xiu-guang[1,3]

(1. Key Laboratory of Network & Information Security under the Chinese Armed Police Force,
Electronic Department, Engineering College of Armed Police Force, Xi'an 710086, China;
2. Key Laboratory of Network & Information Security of the Ministry of Education, Xidian University, Xi'an 710071, China;
3. Institute of Information Security, Engineering College of Armed Police Force, Xi'an 710086, China)

【Abstract】The traditional steganography methods with Pixel Value Differencing(PVD) usually only deal with the PVD in the horizontal direction but ignore the vertical one. In this paper, the cover image is divided into 2×2 nonoverlapping blocks, then the modulus function method is used in horizontal direction and the simple PVD method is used in vertical direction for steganography. The falling-off-boundary problem is solved. Experimental results show that the proposed approach provides higher stego-image quality, larger embedding capacity, and can against common attacks.

【Key words】Pixel Value Differencing(PVD); steganography; modulus function; embedding capacity

DOI: 10.3969/j.issn.1000-3428.2011.14.041

1 概述

近年来，随着 Internet 的迅速发展和广泛应用，信息安全问题日益突出。隐写技术作为一种新兴技术，已成为信息安全领域的一个重要组成部分。文献[1]提出基于像素差(Pixel Value Differencing, PVD)的方案，该方案利用原始载体图像中 2 个相邻像素值的差的大小来决定嵌入秘密信息的多少，但该方案嵌入容量小，隐写图像质量不高，安全性也不好。文献[2]提出一种基于模函数的方案，能明显提高隐写图像的质量，同时抵抗文献[3]的攻击，但其嵌入容量有限。文献[4]提出在水平和垂直方向都嵌入数据的方法，但其采用简单 PVD 方法[1]进行嵌入，不仅嵌入容量低、安全性差，而且图像质量不高。综合文献[1-2, 4]的特点，本文提出一种基于像素差和模函数的隐写方法。

2 相关算法介绍

2.1 原始的 PVD 方案

原始的 PVD 方案[1]思想为：在空域将载体图像分成不相交的小块，每个小块由 2 个相邻像素组成。令小块中的像素灰度值为 P_i 和 P_j，则 $d=P_j-P_i$，$|d|$的取值范围为[0, 255]，将这个范围分成 r 个区域 R_k (k=1,2,…,r)，每个区域的宽度都是 2 的整数幂，如果 d 落在区域 R_k，那么在这个小块中嵌入 $n=\mathrm{lb}(w_k)$ 比特秘密信息，其中，W_k 为第 k 个区域的宽度，在下文中嵌入比特数的计算也用此式。

2.2 基于模函数的 PVD 方案

文献[2]将载体图像分成连续不相交的像素对，b 为秘密信息的十进制值，计算：

$$F_{\mathrm{rem}}=(p_i+p_j)\bmod(2^n) \tag{1}$$

具体嵌入算法详见文献[2]。提取秘密信息时，计算每个像素对可嵌入比特数 $n=\mathrm{lb}(w_k)$，然后用式(1)计算出 F_{rem} 即为嵌入信息的十进制值，最后将十进制的 F_{rem} 转换成 n 比特的秘密信息。

3 基于像素差和模函数的隐写方法

本文方案的基本处理单元为 2×2 的像素块，水平方向的 2 对像素对使用文献[2]中的方法进行嵌入，对垂直方向的一对像素利用文献[1]中的方法进行嵌入。为了能正确提取水平方向的秘密信息，需对垂直方向的另一对像素进行修改；若出现越界情况，则要进行调整；若调整后仍出现越界，则该像素块垂直方向上不嵌入信息，将该块信息利用文献[5]中方法嵌入到图像的最后若干行像素中。

3.1 嵌入算法

嵌入算法的具体步骤如下：

(1)将原始图像按从左到右、从上到下的顺序分成 2×2 的互不相交的像素块，令 M、N 为图像的长和宽，则这样的块

基金项目：国家自然科学基金资助项目(60842006)；武警部队科研基金资助项目(wjk2009020)

作者简介：李 军(1987－)，男，硕士，主研方向：信息隐藏；潘 峰，副教授；李秀广，讲师

收稿日期：2011-01-10 **E-mail：**lijun9250lj@163.com

总共有 $n_{\text{blocks}}=\lfloor M/2\rfloor\times\lfloor N/2\rfloor$ 个，记块中像素(像素值)分别为 A、B、C、D，如图 1 所示。相邻像素差 PVD 的取值范围与 2.1 节一致。

A	B
C	D

图 1 2×2 像素块示例

(2)计算 $d_1=|B-A|$，所属区域为 R_{d1}，嵌入比特数为 n_1；$d_2=|D-C|$，所属区域为 R_{d2}，嵌入比特数为 n_2。利用文献[2]中模函数的方法分别对像素对 AB 和 CD 嵌入信息，记嵌入后的像素值为 A_1、B_1、C_1、D_1。

(3)计算 $d_3=C_1-A_1$，所属区域为 R_{d3}，能嵌入比特数为 n_3；$d_4=D_1-B_1$，所属区域为 R_{d4}，能嵌入比特数为 n_4；如果 $n_3\leqslant n_4$，则选择 A_1C_1 作为垂直方向的像素对利用文献[1]中方案进行嵌入，否则选择 B_1D_1 进行嵌入。为了能正确提取水平方向的秘密信息，需对另一垂直像素对进行调整。不失一般性，以选择 A_1C_1 嵌入为例，记嵌入后的值为 A_2C_2，则按下式将 B_1D_1 调整为 B_2D_2:

$$B_2=B_1-(A_2-A_1) \tag{2}$$

$$D_2=D_1-(C_2-C_1) \tag{3}$$

如果 B_2D_2 都没有越界，则嵌入过程结束，否则进入步骤(4)。

(4)如果 B_2D_2 越界，则选择 $n=\max(n_1,n_2)$，目的是在下面的步骤中 4 个像素同加或同减 $2^n/2$ 后，像素对 A_2B_2 与 C_2D_2 按式(1)计算后结果不变，而 A_2C_2 也保持了相同的像素差:

1)若 $B_2<0\,\|\,D_2<0$，$A_2=A_2+2^n/2$，$B_2=B_2+2^n/2$，$C_2=C_2+2^n/2$，$D_2=D_2+2^n/2$，如果 $A_2B_2C_2D_2$ 仍越界，进入(C);

2)若 $B_2>255\,\|\,D_2>255$，$A_2=A_2-2^n/2$，$B_2=B_2-2^n/2$，$C_2=C_2-2^n/2$，$D_2=D_2-2^n/2$，如果 $A_2B_2C_2D_2$ 仍越界，进入(C)。

标记此块为垂直不可用块，与文献[4]不同，本文方案中选择图像的最后 $2x$ 行来嵌入有关垂直不可用块的信息，该信息格式的顺序为 x 的值(x 由不可用块的总数决定)、总的垂直不可用块数、第 1 个垂直不可用块的标号、第 2 个，一直到最后一个。行数、总数和每一个标号都用 $\text{lb}(n_{\text{blocks}})$ 个比特来表示，采用文献[5]中修改的 3-LSB 方案从图像最后一个像素开始逆序嵌入。

3.2 提取算法

提取秘密信息时，先对图像的最后 $2x$ 行提取垂直不可用块信息，而对其余的 2×2 像素块提取秘密信息，提取过程如下:

(1)逆序提取最后 $2x$ 行像素最低 3 bit 信息，以 $\text{lb}(n_{\text{blocks}})$ bit 作为一个处理单元，每个单元的含义与嵌入相同。如隐写图像为 512×512 像素，则每个处理单元的比特数为 16，假若提取的信息为:

0000000000000001000000000000000100000101000010000

则此隐写图像中使用了 2 行来嵌入垂直不可用信息(即 x=1)，共有不可用块数为 1，编号为 1288。

(2)对每一个秘密信息块，记像素值为 $A_2B_2C_2D_2$，首先将水平 2 对像素 A_2B_2 与 C_2D_2 利用文献[2]中的方法提取出秘密信息，如果该块不是垂直不可用块，则计算 $d_3=C_2-A_2$，$d_4=D_2-B_2$，相应的嵌入容量分别为 n_3 与 n_4，若 $n_3\leqslant n_4$ 则说明在 A_2C_2 嵌入了信息，否则说明在 B_2D_2 嵌入了信息，根据文献[1]中方法提取出秘密信息。如果该块是垂直不可用块，则该块在垂直方向没有嵌入信息。

4 实验结果及分析

对本文方案进行仿真实验，实验所用图像为 512× 512 像素的标准灰度图像，实验数据均为多次实验的平均值。通常隐写方案的评判标准有容量、视觉质量[6]、安全性等，本文也将从这 3 个方面进行实验对比及分析。本文方案与文献[1]方案及文献[4]方案在容量和峰值信噪比(Peak Signal to Noise Ratio, PSNR)上的对比如表 1、表 2 所示。

表 1 本文方案与文献[1]方案的对比

载体图像	文献[1]方案		本文方案		
	容量/bit	PSNR/dB	容量/bit	PSNR/dB	垂直不可用块数
Lena	409 752	39.2	608 704	44.3	0
Peppers	397 850	39.8	606 673	43.9	0
Airplane	397 912	42.2	612 644	43.7	0
Baboon	457 168	37.0	678 954	40.9	9
Couple	412 824	40.2	611 308	43.6	25
Boat	421 080	38.9	617 789	42.8	0
Elaine	408 592	41.9	600 296	45.6	0
Man	423 560	39.1	624 027	43.5	7

表 2 本文方案与文献[4]方案的对比

载体图像	文献[4]方案		本文方案	
	容量/bit	PSNR/dB	容量/bit	PSNR/dB
Lena	593 034	39.18	608 704	44.3
Baboon	600 410	35.11	678 954	40.9
Airplane	590 800	38.05	612 644	43.7
Peppers	578 899	39.80	606 673	43.9

从表 1 可以看出，垂直方向不可用块的数量很少，说明本文方案采用的将垂直方向不可用块信息嵌入在图像的最后 $2x$ 是可行的，而 x 通常为 1。由表 1、表 2 可知，本文方案比文献[1]中方案嵌入容量平均要多 50%左右，且 PSNR 值也大 3 dB~4 dB；与文献[4]方案嵌入容量大致相同，PSNR 值平均大 5 dB 左右。

像素差直方图分析结果如图 2 所示。利用文献[3]中像素差值直方图分析方法对文献[1, 4]进行分析，直方图存在明显阶梯，可知有秘密信息的嵌入；而本文方案的像素差值直方图与原图基本一致，没有阶梯出现，即该攻击对本方案失效。

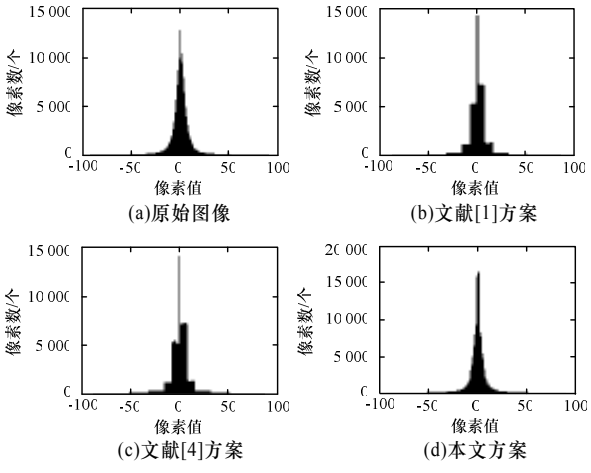

图 2 像素差直方图分析

利用本文方案嵌入秘密信息前后的 Lena 图像对比如图 3 所示。可以看出，嵌入后的图像在视觉上人眼看不出有异常。

(a)嵌入前 (b)嵌入后

图 3 Lena 图像嵌入信息前后对比

图 4 为利用本文方案对 Lena 图像嵌入信息后进行的 RS 隐写分析，将一幅图像分割成互相不重合的像素组。然后用一个区别函数计算每个像素组的规整性。通过这个区别函数以及它的逆函数，将像素组分成 3 类，分别为 Regular、Singular 以及 Unusable。2 个互补的掩码用来模拟加上不同的噪声。使用掩码 m 条件下，Regular 像素组的个数用 R_m 来表示，Singular 像素组的个数用 S_m 来表示，单位均为占总像素组的百分比。可以看出其中的 $R_m \cong R_{-m}$，$S_m \cong S_{-m}$，根据 RS 分析的判断方法可知，本文方案对 RS 攻击免疫。

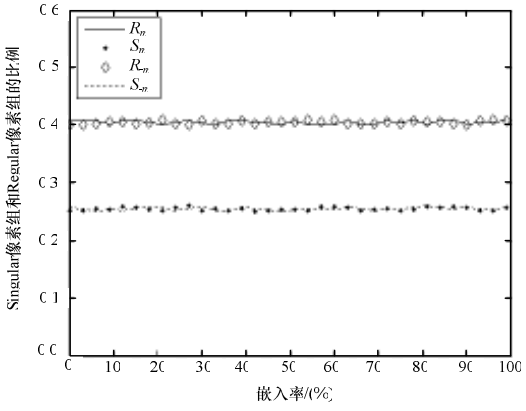

图 4 Lena 隐写图像的 RS 分析结果

5 结束语

本文提出了一种利用水平像素差和垂直像素差的图像隐写方法，利用像素差来嵌入秘密信息。实验证明，本文方案比文献[1, 4]的方案具有更高的嵌入容量和更好的隐写图像质量，而且安全性较高，能抵抗常用的像素差值直方图攻击和 RS 攻击，具有实际应用价值。由于本文算法的嵌入容量较大，因此只能抵抗一些较常用、维数较低的隐写分析，下一步将考虑利用最小嵌入失真原理提高算法的绝对安全性。

参考文献

[1] Wu Da-Chun, Tsai Wen-Hsiang. A Steganographic Method for Images by Pixel Value Differencing[J]. Pattern Recognition Letters, 2003, 24(9): 1613-1626.

[2] Wang Chung-Ming, Wu Nan-I, Tsai Chwei-Shyong, et al. A High Quality Steganographic Method with Pixel Value Differencing and Modulus Function[J]. Journal of Systems and Software, 2008, 81(1): 150-158.

[3] Zhang Xinpeng, Wang Shuozhong. Vulnerability of Pixel Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security[J]. Pattern Recognition Letters, 2004, 25(3): 331-339.

[4] 卜 珑, 胡 波. 一种改进的利用像素差值的数据隐藏方法[J]. 电路与系统学报, 2006, 11(3): 9-13.

[5] Chan Chi-Kwong, Chen Lee-Ming. Hiding Data in Images by Simple LSB Substitution[J]. Pattern Recognition, 2004, 37(3): 469-474.

[6] 郑江云, 江巨浪. 基于感觉容量的图像质量评价算法[J]. 计算机工程, 2010, 36(8): 222-223.

编辑 顾姣健

(上接第 124 页)

```
}
else return (“拒绝操作”);
}
else return (“拒绝操作”);
}
```

关于算法的说明如下：

(1)subject 为主体，是已注册的用户；target 为目标，是指需要访问的 XML 文档；path 为路径，用于指定 XML 文档树中的某一节点，可由 XPath 确定。由目标所指定的 XML 文档及由路径所指定的节点确定了被保护的对象；type 为主体的操作类型，是集合{read (读), write (写)}中的一个元素；

(2)Step1 中 getSubLabel()函数从 Ulabel.xml 中取出主体的安全标签；

(3)Step3 中 getObjLabel()函数从信息安全规则库中取出客体的安全标签；

(4)Step5 中 InRange()函数判断主体请求操作的客体是否在主体的操作范围内；IsValid()判断操作后的文档是否有效。update()函数更新 XML 文档。

5 结束语

XML 应用越来越广泛，对 XML 文档中不同程度的敏感信息实施细粒度的访问控制显得十分必要。本文利用高安全等级系统中最常用的 BLP 模型实现对 XML 文档的安全访问控制。首先在 BLP 模型的基础上，对主体和客体的安全标签进行改进，提出 EBLP(Extended Bell-La Padula)模型，并讨论该模型下安全标签分配。最后讨论该模型的体系结构并给出访问控制算法。在今后的工作中将对多级 XML 文档中的多实例特性及 EBLP 模型实现的细节做进一步的研究。

参考文献

[1] World Wide Web Consortium. Extensible Markup Language Version1.0[EB/OL]. (2004-02-04). http://ww-w.w3.orgTR/REC-xml/.

[2] 薛 凯, 崔杜武, 崔颖安, 等. 基于 XML 与数据库技术的权限管理[J]. 计算机工程, 2009, 35(20): 148-150.

[3] 黄 刚, 王汝传, 田 凯. 基于 RBAC 策略的可信网格控制模型[J]. 计算机应用研究, 2010, 27(4): 1473-1476.

[4] Fan Wenfei, Garofalakis M. Secure XML Querying with Security Views[EB/OL]. (2004-02-02). http://en.scientificcommons.org/42618183.

[5] Bell D E, La Padula L J. Security Computer Systems: Mathematical Foundations and Model[EB/OL]. (1974-10-22). http://portal.acm.org/citation.cfm?id=356852.

[6] World Wide Web Consortium. XML Path Language 2.0[EB/OL]. (2007-01-23). http://www.w3.org/TR/xpath20/.

[7] 李 斓, 何永忠, 冯登国. 面向 XML 文档的细粒度强制访问控制模型[J]. 软件学报, 2004, 15(10): 1528-1537.

编辑 陈 文