

PVD图像隐写算法的安全分析及改进^{*}

黄文婷，方艳梅，黄继武

(中山大学电子与通信工程系 // 信息安全技术广东省重点实验室，广东 广州 510275)

摘 要：PVD (Pixel value differencing 像素差值) 隐写算法具有嵌入容量高和不可见性好的优点。但原始的 PVD 算法容易受到直方图分析的攻击。为提高安全性而提出的修正算法，仍然存在不足。基于对原始和修正 PVD 算法的分析，提出了 PVD 改进算法，在保持 PVD 算法优点的同时，提高了掩密图像的 PSNR 值，并增强了 PVD 算法抵御差分直方图分析攻击的能力。

关键词：隐写；隐写分析；像素差值；直方图分析；安全性

中图分类号：TP391 **文献标识码：**A **文章编号：**0529-6579 (2007) 06-0039-05

隐写术是信息隐藏中的一个重要分支^[1]，安全性和嵌入容量是衡量隐写算法性能的两个重要指标^[2]。但目前隐写术却面临着隐写分析的攻击与挑战^[3-5]。在针对空域的图像隐写算法中，经典的 LSB (the least significant bits 最低比特位) 算法嵌入容量不高，一般不超过 13%^[6]。而目前已有不少成熟分析方法攻击 LSB 隐写算法，如 Chi-square 统计攻击、RS 方法、样本对方法等^[7-9]。PVD (Pixel value differencing 像素差值) 隐写算法利用了人眼对不同条件下的灰度改变有不同敏感度的特点^[10-11]，获得了较高的嵌入容量和不可见性。然而，原始的 PVD 算法不能抵御差分直方图分析攻击。现有针对这一安全漏洞提出的修改算法^[12]，差分直方图的修正效果但仍然不够理想，而且带来了 PSNR 值降低的负面效应。

本文分析了 PVD 算法的安全漏洞以及修改算法中导致 PSNR 值降低的原因，并在现有基础上对算法进行再改进，在保留了其高不可见性及高嵌入容量的同时，消除了 PSNR 值降低的负面效应，并增强了 PVD 算法抵御差分直方图攻击的能力，提高了安全性。

1 PVD 算法的安全分析

1.1 现有的 PVD 算法

PVD 算法最初由 Wu 等^[10]提出，本文将其记为原始算法 (O_PVD)。它用式 (1) 计算出掩密图像各像素对块的 PVD 值从而进行信息嵌入及提取^[10]：

$$d' = \begin{cases} l + b & d \geq 0 \\ -(l + b) & d < 0 \end{cases} \tag{1}$$

其中 l 和 u 是像素对灰度绝对差值 $|d|$ 所属区域的下限 ($k \in \{1, 2, 3, \dots, K\}$)^[10]， l 为待嵌入信息对应的十进制数。

在 Wu 的原始算法的基础上，Zhang 等^[12]对原始算法作了修改，本文将其记为修改算法 (M_PVD)。其方法是在每个像素对块引入一个根据已知密钥产生的在 $[0, 1]$ 内取值的伪随机参数 β ^[12]，并根据

$$\begin{aligned} l_i &= l + \lfloor \beta \cdot w_i \rfloor \\ u_i &= l_{i+1} + \lfloor \beta \cdot w_{i+1} \rfloor - 1 = u + \lfloor \beta \cdot w_{i+1} \rfloor = \\ & \quad l_{i+1} - 1, \quad (i = 1, 2, 3, \dots, K) \end{aligned} \tag{2}$$

得到动态划分的区域上下限 l_i 和 u_i 以及对应可嵌入的比特数 w_i 。与原始算法的式 (1) 相对应，M_PVD 算法用式 (3) 或 (4) 计算掩密图像各像素对块的 PVD 值，再进而嵌入及提取信息^[12]：

若 $|d| \in [l_i, u_i]$

$$d' = \begin{cases} \begin{aligned} & \arg \min_{l_k \leq u_k \bmod \{w_k\} = b} (|e - d|), & d \geq 0 \\ & - \lceil \begin{aligned} & \arg \min_{l_k \leq u_k \bmod \{w_k\} = b} (|e - d|) \rceil, & d < 0 \end{aligned} \end{aligned} \end{cases} \tag{3}$$

若 $|d| \in [0, u_0]$ ，则

$$d' = \begin{aligned} & \arg \min_{-u_0 \leq u_0 \bmod \{w_0\} = b} (|e - d|) \end{aligned} \tag{4}$$

1.2 PVD 算法的安全分析

Wu 等提出的 O_PVD 算法计算简单，嵌入容

^{*} 收稿日期：2006-12-01
基金项目：广东省自然科学基金资助项目 (04205407 05300907)；模式识别国家重点实验室开放基金资助项目
作者简介：黄文婷 (1984 年生)，女，硕士研究生；通讯联系人：方艳梅，E-mail: fangym@mail.sysu.edu.cn
(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

量大，但是却存在安全漏洞，不能抵御直方图分析的攻击。经 O_PVD 算法隐写的掩密图像的差分直方图会出现如图 1 (a) 所示的“阶梯效应”^[12]，暴露了秘密信息的存在，甚至可被用来估计掩密图像所含秘密信息的长度。

对 O_PVD 算法的安全漏洞做出修正的 M_PVD 算法^[12]，直方图修正效果如图 1 (b) 所示。可

见，与载体图像相比，掩密图像的 PVD 直方图在主峰两侧仍然存在异常的波动。而且， M_PVD 算法也带来了 PSNR 值降低和嵌入容量轻微损失的负面效应，如表 1 所示。 M_PVD 算法嵌入容量减少的主要原因是重新划分区间导致了可用块数的减少，但总体上嵌入率降低很小，可以忽略不计。

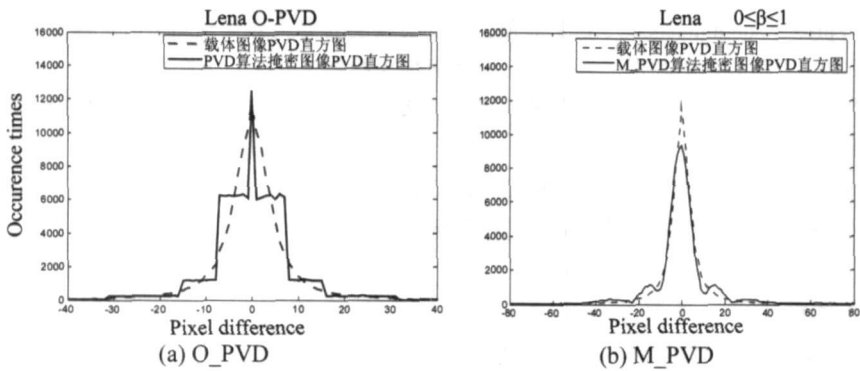


图 1 O_PVD 和 M_PVD 算法的原始图像及掩密图像的差分直方图 (Lena)
Fig 1 The Pixel difference histograms of original Lena and stego Lena of O_PVD and M_PVD

表 1 O_PVD 与 M_PVD 算法性能比较 (Lena)

Tab 1 Comparison between the O_PVD and M_PVD methods (Lena)

算法	嵌入容量 /bits	嵌入率 /%	PSNR/ dB
O_PVD	409802	19.54	41.07
M_PVD	403665	19.25	38.55

下面分析 M_PVD 算法中造成 PSNR 值降低的原因。根据式 (2) 的方法动态划分新区域，是将区域的上下边界 l 和 u 按 β 随机向数轴的正方向随机移动一段距离并拉伸区域宽度。因 β 只取正值，区域不能向数轴负方向平移，对于同一个像素块，由 M_PVD 算法得到的新 PVD 值 d 的取值范围 $[l', u']$ 与 O_PVD 算法的固定区域 $[l_k, u'_k]$ 相比，会在 $[l_k, l'_k]$ 产生空洞。为了方便比较，把 O_PVD 算法中由式 (1) 调整得到的 d' 记为 d'_0 ， M_PVD 算法中由式 (3) 或 (4) 调整得到的 d 记为 d'_M ， d'_M 的取值范围在 $[l', l'_k]$ 产生空洞，也就是说， d'_M 无法在区域 $[l_k, l'_k]$ 内取值。当 d'_0 与 d'_M 分别落在区域 $[l_k, l'_k]$ 与 $[l'_k, l'_k]$ 内时，则有 $|d - d'_0| \leq |d - d'_M|$ ，从而造成了 M_PVD 算法的 PSNR 值比 O_PVD 算法有所降低。 β 的取值范围越大，则空洞 $[l_k, l'_k]$ 的宽度越大， d 与 d'_M 分别落在 $[l_k, l'_k]$ 和 $[l'_k, l'_k]$ 内的概率越大， d'_M 远离 d 的可能性越大，从而导致 PSNR 值降低得越多。

实际上，不论取何值，都有 $|d - d'_0| \leq |d - d'_M|$ ，根据式 (3) 以及 PSNR 值的计算方法，空洞 $[l_k, l'_k]$ 的存在致使 $|d - d'_0| \leq |d - d'_M|$ ，是 M_PVD 算法的 PSNR 值比 O_PVD 算法有所降低的主要原因，也导致掩密图像的 PVD 直方图仍然存在波动。

2 PVD改进算法

本文提出的 PVD 改进算法 (记为 I_PVD)，对 M_PVD 算法中新区域划分的方法进行调整，使新区域能动态地向数轴的正负方向随机调整。取 β 属于 $[-4, +4]$ 之间的整数，按

$$l_i = l_i + \beta, u'_i = u'_i + \beta \tag{5}$$

进行新的区域划分，找到 $|d|$ 所属的区域边界 l'_k 和 u'_k ，然后把 l'_k, u'_k 代入到式 (3) 或 (4) 计算 d' 进行嵌入。

这时，新区域的宽度为

$$w'_i = u'_i - l'_i + 1 = (u_i + \beta) - (l_i + \beta) + 1 = u_i - l_i + 1 = w_i \tag{6}$$

与原来固定划分的区域的宽度相等，能嵌入 $\log_2 w_k$ 入比特的信息。实际上，这种改进方法是将原来全部固定划分的区域为整体，按照 β 的值，随机向数轴的正方向或者负方向平移一段距离，如图 2 所示。

由以上分析可见，新划分的区域仍然是连续且互不交叠的，嵌入前后的 d 和 d' 能唯一映射到某个区域 R_k ，因此能实现盲提取。而且，由于区

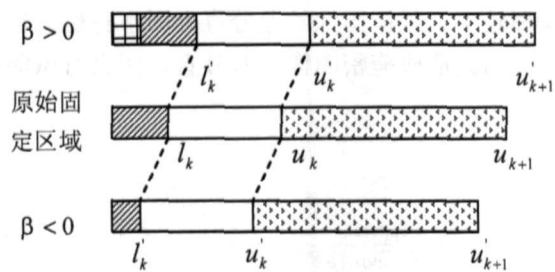


图 2 I_PVD算法区域动态划分示意图
Fig 2 The dynamic division of the ranges of I_PVD method

域能向数轴的正负两个方向进行动态调整, 因此能够有效降低在 $[l_k, l_k]$ 形成空洞的概率。这样, 既能有效消除由于区域边界 l_k 和 u_k 固定而引起的阶梯效应, 又不会因为只朝一个方向动态移动拉伸而造成 PSNR 值的降低。对于 Lena 图像, 隐写后得到的像素差值直方图如图 3 所示, 可见 I_PVD 算法能够有效消除 M_PVD 算法中直方图的波动。

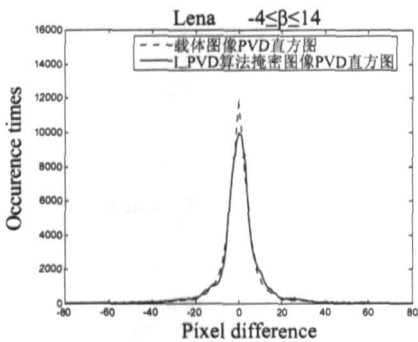


图 3 载体图像和 I_PVD 算法掩密图像差
分直方图的对比 (Lena 图像)

Fig 3 The pixel difference histograms of original Lena and
stego Lena of O_PVD and I_PVD

Lena 掩密图像在 β 取不同范围时 PSNR 比较分析如表 2 所示。可见, 当 β 的取值范围较小时, I_PVD 算法的 PSNR 值比 O_PVD 算法有所提高; 随着 β 取值范围的增大, PSNR 降低得愈多。这是由于, 取值范围越大, 即区域划分的动态调整范围越大, 虽然越有利于阶梯效应的消除; 但 β 越大, 动态区域则越偏离原来的固定区域, 远离 d_k 的可能性越高, PSNR 值不但没有提高, 反而降低。嵌入容量方面, 虽然 I_PVD 算法与 O_PVD 算法相比有轻微的降低, 但由于 β 的动态范围不足以改变“可用块”的数量, 所以 β 的取值范围基本不影响嵌入容量。权衡 PSNR 值和直方图分析的效果后, 取 $\beta \in [-4, 4]$ 。由于 $|\beta| \leq 4 = \frac{1}{2} \min(w_i)$, 即新的动态区域偏离原始固定区域最多不会超过区

域宽度的一半, 则使区域有一定动态范围的同时, 不会偏离原固定区域太大以致降低 PSNR 值。

表 2 O_PVD 和 I_PVD 算法性能比较 (Lena 图像)
Tab 2 Comparison between the O_PVD and I_PVD methods

算法	嵌入容量 / bits	嵌入率 / %	PSNR / dB
O_PVD	409802	19.54	41.07
I_PVD	$\beta \in [-2, 2]$	19.39	41.93
	$\beta \in [-4, 4]$	19.39	41.43
	$\beta \in [-6, 6]$	19.39	40.86
	$\beta \in [-8, 8]$	19.38	39.80

3 实验结果

3.1 隐写算法实验结果

以 $512 \times 512 \times 8$ bits 的 Lena, Peppers, Boat 和 Baboon 灰度图像为载体图像, 分别用改进前后的三种 PVD 算法进行满嵌入的比较测试, 统计结果如表 3 所示。从表 3 可见, 对于同一幅载体图像, O_PVD 算法的嵌入率最高, I_PVD 算法次之, M_PVD 算法最低, 但是差别不大, 只在 0.1% ~ 0.5% 范围内。这是由于 M_PVD 算法和 I_PVD 算法调整了按灰度值划分的区域边界, 使可用小块的数量减少而造成的。在 PSNR 值方面, 对同一幅载体图像, M_PVD 算法比 O_PVD 算法的 PSNR 值降低了 3 dB 左右, 而 I_PVD 算法则比 O_PVD 算法有 0.17 ~ 0.7 dB 的提高, 由此可见 I_PVD 算法有更好的性能和实用价值。

表 3 O_PVD, M_PVD 及 I_PVD 隐写算法的性能比较
Tab 3 Comparison among the O_PVD, M_PVD and I_PVD methods

图像	嵌入率 / %			PSNR / dB		
	O_PVD	M_PVD	I_PVD	O_PVD	M_PVD	I_PVD
Lena	19.54	19.25	19.39	41.07	38.55	41.43
Peppers	19.33	18.88	19.08	41.60	39.36	41.76
Boat	19.93	19.42	19.65	39.80	36.97	40.46
Baboon	21.79	20.79	21.27	36.91	33.16	37.45

3.2 性能分析

3.2.1 直方图分析攻击 直方图分析, 是针对图像的 PVD 值分布的直方图的分析, 且其中像素对划分方法与隐写时相同。Lena, Peppers, Boat 和 Baboon 四幅载体图像经 I_PVD 算法隐写后的掩密图像 PVD 直方图与载体图像 PVD 直方图的比较分析分别如图 4 (a) — (d) 所示。

由图 4 可以看到, I_PVD 算法的掩密图像的 PVD 直方图能很好的拟合载体图像的 PVD 直方图, 阶梯效应和波动都已经全部消除, 能够有效的抵御

直方图分析的攻击。但由于 PVD算法与图像像素差值密切相关，图像的纹理不同，差分直方图的形状也会有所区别。如图 4（d），因 Baboon图像本

身纹理较多，载体图像的差分直方图本身也比较不平滑，因此造成掩密图像的差分直方图也有微弱的波动。

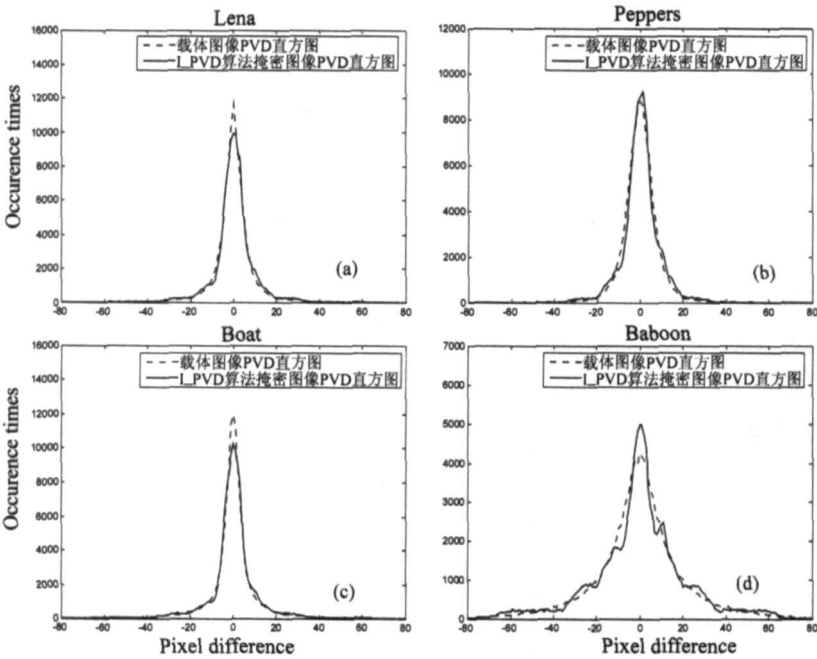


图 4 I_PVD算法掩密图像与载体图像的 PVD直方图的比较分析

图 4 The pixel difference histograms of cover images and the stego-images of I_PVD method
(a) Lena; (b) Peppers; (c) Boat; (d) Baboon

3.2.2 RS分析攻击 RS分析是由 Fridrich^[8]提出的隐写分析方法，参数 I 是判断秘密信息是否存在的依据。 I 值若接近 1，则可判断为有秘密信息的存在， I 值若大于 1，则判断为满嵌入； I 值如果很小或者为负，则判断为不含任何秘密信息。对用不同算法隐写得到的掩密图像进行 RS分析，得到的 I 值如表 4 所示。可见，所有的 I 值都非常接近 0，都被判断为“不含秘密信息”，即无论是原始的 PVD算法还是改进后的 PVD算法，都能够抵御 RS分析的攻击。

表 4 O_PVD、M_PVD及 I_PVD算法掩密图像 RS分析 I 值统计表

Tab. 4 The statistics of RS analysis to O_PVD, M_PVD and I_PVD methods

图像	O_PVD	M_PVD	I_PVD
Lena	0.009 267 4	-0.023 549	-0.020 03
Boat	-0.003 707 1	0.002 092 6	0.021 004
Peppers	0.018 288	0.027 338	0.010 468
Baboon	-0.034 272	-0.166 93	0.009 503 6

4 结 论

本文对一种利用人眼对灰度改变的敏感度的 PVD隐写算法进行了安全漏洞分析和改进。本文所提出的改进 PVD算法，与现有 PVD算法相比，有以下优势：

（1）能有效抵御直方图分析。本文算法的掩密图像的 PVD直方图能很好的拟合载体图像的 PVD直方图，阶梯效应和异常波动都已经基本消除。

（2）PSNR性能得到改善。本文算法解决了 M_PVD算法中 PSNR值降低的问题，PSNR值有 0.17~0.7 dB左右的提高，使掩密图像获得更好的不可察觉性。

此外，本文所提出的改进 PVD算法仍保持了原始 PVD算法嵌入率高的优点，嵌入率平均能够达到 20%。本文的改进算法与原始算法相比，嵌入容量只有 0.1%数量级的降低，基本不影响算法的性能。

参考文献:

[1]

PETITCOLAS F A P ANDERSON R J KUHN M G Information hiding a survey [J]. Proceedings of the IEEE 1999 87 1062—1078

[2]

CHANDRAMOULI R KHARRAZ M MEMON N Image steganography and steganalysis: concepts and practice [J]. Lecture Notes in Computer Science 2004 2939 35—49

[3]

JOHNSON N JAJODIA S Steganalysis of images created using current steganography software [J]. Lecture Notes in Computer Science 1998 1525 273—289

[4]

FRIDRICH J GOLJAN M Practical steganalysis of digital images—state of the art [J]. Security and Watermarking of Multimedia Contents IV Proc SPIE 2002 4675 1—13

[5]

CHANDRAMOULI R SUBBALAKSHMI K P Current trends in steganalysis: a critical survey [J]. IEEE Conf on Control Automation Robotics and Vision ICARCV Kunming China 2004 2 964—967

[6]

SALLEE P Model-Based steganography [J]. Lecture Notes in Computer Science Springer 2004 2939 154—167

[7]

WESTFELD A PFITZMANN A Attacks on steganographic systems [J]. Lecture Notes in Computer Science 1999 1768 61—76

[8]

FRIDRICH J GOLJAN M DU R Detecting LSB steganography in color and gray-scale images [J]. IEEE Multimed Mag October–December 2001 8(4): 22—28

[9]

DUMITRESCU S WU X WANG Z Detection of LSB steganography via sample pair analysis [J]. IEEE Trans on Signal Processing 2003 51(7): 1995—2007.

[10]

WU D TSAI W A Steganographic method for images by pixel value differencing [J]. Pattern Recognition Letters 2003 24 1613—1626

[11]

WU D TSAI W Spatial-domain image hiding using image differencing [J]. Vision Image and Signal Processing EE Proceedings 2000 147(1): 29—37.

[12]

ZHANG X WANG S Vulnerability of pixel value differencing steganography to histogram analysis and modification for enhanced security [J]. Pattern Recognition Letters 2004 25 311—339

Security Analysis and Improvement of the PVD-based Image Steganography

HUANG Wen ting FANG Yan mei HUANG Ji wu
(Department of Electronic and Communication Engineering// Guangdong Key Laboratory of Information Security Technology Sun Yat sen University Guangzhou 510275 China)

Abstract: The pixel value differencing (PVD) steganography has the superiority of high capacity and good imperceptibility, but the original PVD method is vulnerable to histogram analysis. A modified PVD method was proposed to enhance the security, the deficiency still exists. Basing on the analysis of the original and modified PVD method, an improved PVD algorithm is proposed. While preserving the superiority of PVD method, the improved method increases the PSNR and the histogram analysis immunity.

Key words: steganography, steganalysis, pixel value differencing, histogram analysis, security