一种空域 BPCS 信息隐藏的改进算法

卜 毅 曹汉强
(华中科技大学电子与信息工程系,武汉 430074)

摘 要 针对位平面复杂度分割密写易受复杂度直方图攻击的问题,提出了一种密写改进算法,即用类噪声块一半的像素嵌入秘密信息,另一半用改变像素值的方法来调整区域的整体复杂度,以达到抗攻击的目的。实验结果表明,改进的算法能很好的抵抗复杂度直方图攻击。

关键词 信息隐藏 密写 位平面复杂度分割 直方图
中图法分类号: TP911.73 **文献标识码**: A **文章编号**: 1006-8961(2008)03-0406-05

A Modified Algorithm of Spatial BPCS-Steganography

BU Yi, CAO Han-qiang
(*Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan* 430074)

Abstract This paper aimed at solving the problem of using complexity histogram steganalysis to BPCS-steganography (Bit-Plane Complexity Segmentation-Steganography) and presented an improved method. For compensating the BPCS security deficiency, we used a half pixels of "noise-like" block for embedding secret information, and the other half pixels were used for adjusting complexity. Experiment results showed this method can properly counteract the attack of complexity histogram.

Keywords information hiding, steganography, BPCS(Bit-plane complexity segmentation), histogram

1 引 言

信息隐藏技术是信息安全领域一个新兴的研究方向,密写(steganography)技术是信息隐藏的一个重要分支[1],其目的是以图像、音频等数字媒体作为掩护,将要发送的秘密消息嵌入到载体信号内部,以不引起外界注意的方式通过公共信道进行秘密传递。

位平面复杂度分割(Bit-plane complexity segmentation, BPCS)密写是基于复杂度计算的比特位平面分割技术。其主旨是将载体数据的多个位平面都分成固定大小的小块,由于人的感觉器官对那些变化剧烈、复杂度较高的位面小块比较不敏感,所以利用这些位面小块来负载秘密信息[2],具有较好的隐蔽性;另外,秘密信息可以加载在多个位平面,所以有很大的嵌入量。BPCS 密写最初被直接应用于静止图像的空间域,随后该方法的提出者又将其应用于小波压缩域[3,4],根据 BPCS 密写的原理还衍生出了一些新的密写方法[5]。但 BPCS 密写方法也存在安全漏洞,主要原因是嵌入的秘密信息块的复杂度与"类噪声"(noise-like)块不同,将所有的"类噪声"块用秘密信息代替会导致复杂度直方图异常现象,由复杂度直方图的不连续性可以判断秘密信息的存在性[6]。

本文针对空域 BPCS 存在易于判断嵌入秘密信息的问题,提出了一种抗攻击算法,用"类噪声"块一半的像素嵌入秘密信息,另一半用改变像素值的方法来调整区域的整体复杂度,达到抗攻击的目的。

2 BPCS 密写及分析

BPCS 密写法是一种新型的空域密写技术,具

基金项目:国家科技部攻关项目(2004BA811B06);广东省科技攻关项目(2004B10101023)
收稿日期:2006-09-05;**改回日期**:2006-10-24
第一作者简介:卜毅(1982~),男。华中科技大学通信与信息系统专业硕士研究生。主要研究方向为数字图像处理、信息安全的研究。E-mail:itdnet@mail.hust.edu.cn

有较好的隐蔽性和很大的嵌入量。不仅可直接应用于静止图像的空间域,而且可用于变换域中的嵌入。具体的 BPCS 密写方法如下:

(1) 首先将载体图像的所有位平面分成 $m \times m$ 大小相同的小块。

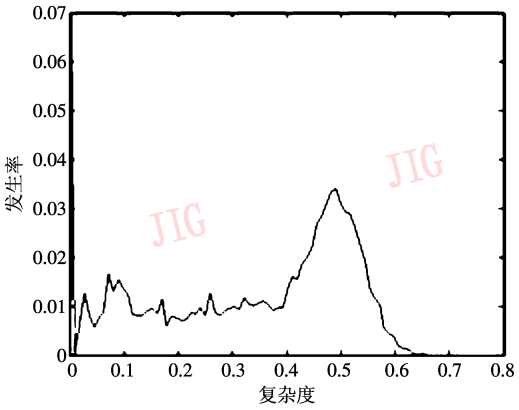
(2) 利用公式 $\alpha = \dfrac{k}{2 \times m \times (m-1)}$ 计算每个小块的复杂度 α。其中,k 表示黑白边界的长度。分母为 $m \times m$ 小块的黑白边界最大长度;一个 8×8 小块的黑白边界最大长度为 112。

(3) 将复杂度 α 大于 α_{TH} 的位面小块定义为"类噪声"块,用于负载秘密信息,其中 α_{TH} 表示判断位面小块是否可嵌入秘密信息的阈值,其值要小于 0.5,例如取为 0.4。

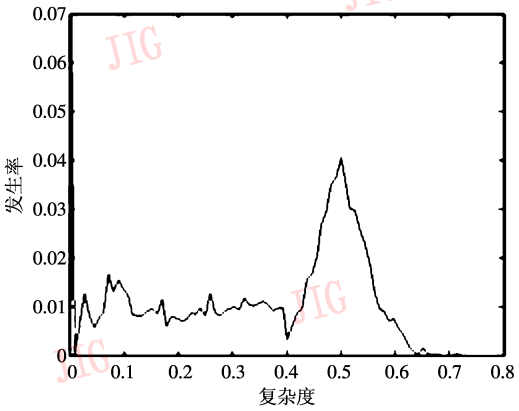
(4) 将嵌入的秘密信息组成 $m \times m$ 大小的位面小块 $\boldsymbol{P}$,如果其复杂度 $\alpha(\boldsymbol{P})$ 大于 α_{TH},直接替换原位面小块;如果其复杂度小于等于 α_{TH},则要作共轭处理,将秘密信息组成的位面小块 $\boldsymbol{P}$ 与 $m \times m$ 大小的棋盘状小块作异或运算生成新的小块 $\boldsymbol{P}^*$,进行共轭运算后有 $\alpha(\boldsymbol{P}^*) = 1 - \alpha(\boldsymbol{P})$,因为 $\alpha \leqslant 0.5$,所以新小块的复杂度一定大于 α_{TH}。然后用新的小块替换原始数据的位面小块,保证了嵌入块的复杂度始终大于 α_{TH}。

(5) 记录下哪些小块是经过共轭处理的,将这部分信息也嵌入到载体数据中。这些额外信息的嵌入不能影响已经嵌入的秘密信息,并且要能够正确提取。

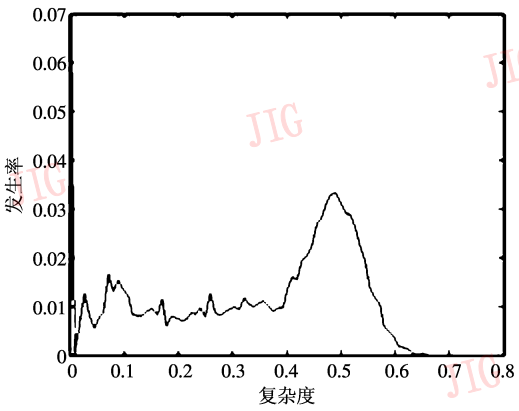
以 256×256 的标准灰度图像 Lena 为例对 BPCS 算法进行分析。将灰度图像分成 8 层,每层按 8×8 分块,分别计算出每个小块的复杂度,然后对原始图像所有位面小块的复杂度进行统计,将其直方图记为 $h_{ORG}(c)$,如图 1(a)所示。用随机序列作为秘密信息进行 BPCS 密写,将位面小块的尺寸取为 8×8,当取阈值 $\alpha_{TH} = 0.4$ 时,嵌入量为 2.5×10^5 bits,密写引起的 PSNR = 28.5dB,嵌入秘密信息后得到的复杂度直方图 $h_{EMB}(c)$,如图 1(b)所示,密写后的直方图在复杂度的值与阈值 α_{TH} 相等处产生了剧烈的变化。直方图在复杂度小于 α_{TH} 变换到等于 α_{TH} 时急剧下降,然后又随着复杂度的变大缓慢上升,出现了明显"山谷现象"。产生这一现象是由于"类噪声"块(用 $\boldsymbol{P}_{ORG}$ 表示)与对应的嵌入秘密信息块(用 $\boldsymbol{P}_{EMB}$ 表示)的复杂度必须满足 $\alpha_{TH} \leqslant \alpha(\boldsymbol{P}_{ORG})$ 和 $\alpha_{TH} \leqslant \alpha(\boldsymbol{P}_{EMB})$,但在满足条件时,并不能保证"类噪声"块的复杂度一直和嵌入信息块的复杂度相等,所以导致了复杂度在 α_{TH} 附近的位面小块的个数急剧减小,大于 α_{TH} 的位面小块的个数变多,密写后图像的复杂度直方图出现"山谷现象"。因此,可以通过对密写后图像的复杂度直方图统计



(a) 由原始图像 Lena 得到的复杂度直方图



(b) 嵌入秘密信息后的图像复杂度直方图



(c) 改进的 BPCS 密写后的图像复杂度直方图

图 1　复杂度直方图

Fig. 1　Complexity histograms

判断出秘密信息的存在性。

3 算法的改进方案

在传统的 BPCS 密写中,秘密信息经过处理后直接置换“类噪声”位面小块,导致产生复杂度直方图异常现象。本文提出的方法中,用“类噪声”块一半的像素进行嵌入,剩下的一半用以调整复杂度。改进方案如下:

将 1 幅二值图像划分为 $m \times m$ 的块,设 $\boldsymbol{P}^i$($i = 1,2,\cdots,N$)为“类噪声”块,$C^i = \alpha(\boldsymbol{P}^i)$,$C^i$ 表示 $\boldsymbol{P}^i$ 的复杂度。

将 $\boldsymbol{P}^i$ 中的像素分为两组,A 组和 B 组,在 A 组像素中嵌入秘密信息,B 组中的像素则用来进行复杂度调整。A 组和 B 组像素的位置与棋盘模块相似,图 2 中给出了 A 组和 B 组像素在位面小块中的位置分配图。

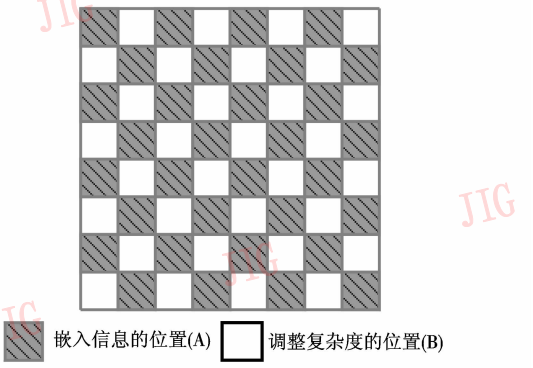


图 2 位面小块各像素位置分配

Fig. 2 Locations assignment of bit-plane

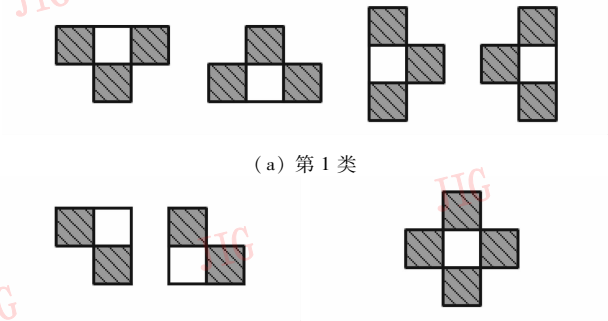
设 $\boldsymbol{P}^i_{\mathrm{A}}$ 表示在 $\boldsymbol{P}^i$ 中 A 组位置嵌入了秘密信息后的小块,C^i_{A} 表示嵌入了秘密信息后小块 $\boldsymbol{P}^i_{\mathrm{A}}$ 的复杂度。

根据位面小块中 B 组像素点的位置归纳为 3 大类,每类分别存在不同的形状,如图 3 所示。当各种形状中 B 组位置的像素值取反时,如果使 $\boldsymbol{P}^i$ 的复杂度变大,则定义该像素点为 B +;反之,则定义为 B -;若复杂度不发生变化则定义为 B0。

不同位置的像素值取反时引起的边界长度变化不同,表 1 中给出了 B 组像素取反后的边界长度改变量以及复杂度变化类别。

改进方案后算法的实现具体步骤如下(以 $\boldsymbol{P}^i$ 块为例,其嵌入秘密信息前复杂度为 C^i):

(1) 将 $m \times m/2$ 大小的二值秘密信息嵌入 $\boldsymbol{P}^i$ 中的 A 组位置,并计算 C^i_{A}。



(a) 第 1 类

(b) 第 2 类 (c) 第 3 类

图 3 调整复杂度像素的位置分类

Fig. 3 Classes of adjusting complexity locations

表 1 B 位置像素值取反

Tab. 1 Reverse the pixels value of B

类别	邻域像素值的和	像素值从 0→1(边界长度的变化/复杂度变化类别)	像素值从 1→0(边界长度的变化/复杂度变化类别)
第 1 类	0	+3/B +	-3/B -
	1	+1/B +	-1/B -
	2	-1/B -	+1/B +
	3	-3/B -	+3/B +
第 2 类	0	+2/B +	-2/B -
	1	0/B0	0/B0
	2	-2/B -	+2/B +
第 3 类	0	+4/B +	-4/B -
	1	+2/B +	-2/B -
	2	0/B0	0/B0
	3	-2/B -	-2/B -
	4	-4/B -	-4/B -

(2) 改变位面小块中 B 组位置像素值,调整目标复杂度 C_{emb},使其等于或最大程度的接近 C^i_{A} 的值。

$\boldsymbol{P}^i$ 的复杂度调整是按以下步骤反复进行的。

如果 $\boldsymbol{P}^i_{\mathrm{A}}$ 满足 $C^i_{\mathrm{A}} < C^i$,则选择一个在 B + 中的像素,将其像素值取反,并从 B + 移出。重复执行这一步骤直到 C_{emb} 大于等于 C^i,或者 B + 为空。

如果 $\boldsymbol{P}^i_{\mathrm{A}}$ 满足 $C^i_{\mathrm{A}} > C^i$,则选择一个在 B - 中的像素,将其像素值取反,并从 B - 中移出,重复执行这一步骤直到 C_{emb} 小于等于 C^i,或者 B - 为空。

如果 $\boldsymbol{P}^i_{\mathrm{A}}$ 满足 $C^i_{\mathrm{A}} = C^i$,则不作任何变化。

(3) 记录经过复杂度调整处理后复杂度小于阈值 α_{TH} 的小块,将这部分信息也嵌入到载体数据中。这些额外信息的嵌入不能影响已经嵌入的秘密信息,并且要能够正确提取。

提取秘密信息时,只需找到复杂度大于 α_{TH} 以及第(3)步中记录的位面小块,然后进行 A 组位置的信息提取即可。

4　实验结果及分析

实验 1

验证本文提出的改进 BPCS 算法的抗复杂度直方图攻击能力。

以 256 × 256 的标准灰度图像 Lena 为例,将灰度图像分成 8 层,由于图像高位平面相邻比特之间的具有很强的相关性,对其进行密写后,高位平面的值将发生改变,图像整体会出现严重的失真,且高位平面的"类噪声"块数量极少,对其不进行密写,图像的总体嵌入量不会有太大变化。所以只对图像的 6 个低位平面进行改进的 BPCS 密写。按本文提出的改进方法,取阈值 $\alpha_{TH} = 0.4$,嵌入量信息量为 1.23×10^5 bits,密写后引起的 PSNR = 38.7dB。如图 4 中(a)、(b)对比所示,改进算法后的密写图像较原始 BPCS 的密写图像失真较小,具有更好的隐蔽性。

(a) BPCS 密写后的图像(PSNR = 28.5dB)

(b) 改进型 BPCS 密写后的图像(PSNR = 38.7dB)

图 4　嵌入秘密信息后的图像对比

Fig. 4　Contrast of the embedded images

图 1(c)为改进型 BPCS 密写后的图像复杂度直方图,可以看出,该图的连续性较好,在复杂度等于阈值 α_{TH} 附近时没有明显的"山谷现象",反而连续性特别好。与原始图像的复杂度直方(图 1(a))相比,复杂度的取值对应的发生率观察不到有太大变化。又对多幅图像 Lena、Baboon、Bridge、Lake、Peppers 等进行测试,使用本文提出的方法均可以有效抵御复杂度直方图的攻击。

实验 2

本文提出的方法与文献[7]提出的方法进行比较。文献[7]中提出的 BPCS 改进算法同样利用到了位平面小块复杂度调整的思路,但其定义"类噪声"块为复杂度大于 α_{TH} 小于 $1 - \alpha_{TH}$ 的位面小块,而且算法上较本文复杂。一般位面小块复杂度越小,像素间的相关性就越强,对其值进行改变时易产生明显的图像失真,尤其是在高位平面,为保证嵌入秘密信息后图像的效果,阈值 α_{TH} 的选取一般在 0.4 ~ 0.5 之间较好。表 2 给出了在 α_{TH} 选取不同值时,两种方法在 256 × 256 的标准灰度图像 Lena 中嵌入量的对比,很明显可以看出,本文提出的算法的嵌入量大于文献[7]方法提出的,而且随着阈值的变大,嵌入量的大小差距越来越明显,对于复杂度较大的图

表 2　嵌入量的比较

Tab. 2　Contrast of the embedded capacities

α_{TH} 的取值	嵌入量	
	本文提出的方法	文献[7]提出的方法
0.40	123 168	110 147
0.42	111 456	96 092
0.44	101 312	78 152
0.46	88 416	45 280
0.48	72 969	30 556
0.49	64 192	20 172

像,本文提出的方法在嵌入量上有更明显的优势。隐蔽性和嵌入量是密写的重要性能指标,取 α_{TH} = 0.4 时,按本文提出方法进行密写后引起的 PSNR = 38.7dB,文献[7]中密写后引起的 PSNR = 39.1dB,而人眼往往不能有效察觉峰值信噪比 38dB 以上的影响[8],说明本文提出的算法和文献[7]的算法一样具有很好的隐蔽性,而且在嵌入量指标上要优于文献[7]的算法。总之,本文提出的改进算法较文献[7]的算法简单、易于实现,在保证嵌入后图像质量的前提下,有更大的嵌入量。

5 结 论

BPCS 密写易受复杂度直方图攻击,本文针对此算法漏洞,提出了一种改进型的 BPCS 密写算法。该算法充分利用了图像复杂度的统计原理,对嵌入信息引起的复杂度变化进行补偿,算法实现简单,具有很强的适应性,实验结果表明,改进的算法具有很好的抗复杂度直方图攻击的能力。

参考文献(References)

1 Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding a survey[J]. In: Proceedings of IEEE, 1999, **87**(7): 1062 ~ 1078.

2 Kawaguchi E, Eason R O. Principle and application of BPCS steganography[A]. In: Proceedings of SPIE Multimedia Systems and Applications[C], Boston, MA, USA, 1998: 464 ~ 472.

3 Spaulding J, Noda H, Shirazi M N, *et al*. BPCS steganography using EZW lossy compressing images[J]. Pattern Recognition Letters, 2002, **23**(13): 1579 ~ 1587.

4 Noda H, Furuta T, Niimi M, *et al*. Application of BPCS steganography to wavelet compressed video[A]. In: Proceedings of International Conference on Image Processing[C], Singapore, 2004: 2147 ~ 2150.

5 Hioki H. A data embedding method using BPCS principle with new complexity measures[EB/OL]. http://www.know.comp.kyutech.ac.jpPSTEG02/Papers/pdf-files/O05-Hioki.pdf.

6 Zhang Xin-peng, Wang Shou-zhong. Statistical analysis against spatial BPCS steganography[J]. Journal of Computer-aided Design and Computer Graphics, 2005, **7**(17):1625 ~ 1629. [张新鹏,王硕中. 对空域 BPCS 的统计分析[J]. 计算机辅助设计与图形学学报, 2005,**7**(17):1625 ~ 1629.]

7 Niimi M, Ei T, Noda H, *et al*. An attack to BPCS-steganography using complexity histogram and countermeasure[A]. In: Proceedings of International Conference on Image Processing[C]. Singapore, 2004: 733 ~ 736.

8 Petitcolas F A P, Anderson R J. Evaluation of Copyright Marking Systems[A]. In: Proceedings of IEEE Multimedia Systems[C], Florence, Italy, 1999: 574 ~ 579.