第34卷 第19期 计 算 机 工 程 2008年10月
Vol.34 No.19 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)19—0179—03 文献标识码：A 中图分类号：TP309

一种改进的位平面复杂度分割算法

娄振华，汤光明
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：对复杂度直方图的不连续性测度的隐写分析能有效地察觉以位平面复杂度分割(BPCS)隐写的秘密信息的存在。为提高隐写算法的安全性，提出一种改进的BPCS算法，即利用部分可嵌入块作为嵌入信息的调节块，消除由于嵌入秘密信息而造成的复杂度直方图的剧烈变化，确保不连续性测度不会出现明显的峰值。实验结果表明，该算法能有效地抵抗基于复杂度直方图的统计分析，同时也保持了原算法嵌入容量大的特点。

关键词：位平面复杂度分割；隐写；复杂度直方图；安全性

Improved Bit-Plane Complexity Segmentation Algorithm

LOU Zhen-hua, TANG Guang-ming
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 Statistical analysis based on complexity histogram discontinuities measure is a powerful steganalytic technique for detecting the presence of secret message embedded in the digital images using Bit-Plane Complexity Segmentation(BPCS). Therefore, to improve steganographic security, this paper proposes an improved BPCS algorithm that can effectively resist statistical analysis. Part of blocks are used that can embed hiding information as complexity adjustable blocks to remove two clearly discontinuities which are caused by customary BPCS algorithm, and make sure the discontinuities measure disappear obviously peak value. Experimental results show that the improved algorithm can effectively resist statistical analysis based on the complexity histogram, and can maintain the big capacity characteristic of the originally algorithm.

【Key words】 Bit-Plane Complexity Segmentation(BPCS); steganography; complexity histogram; security

1 概述

为了提高隐蔽性，有些隐藏算法利用视觉特性进行秘密信息嵌入，即在视觉不敏感的区域嵌入较多秘密信息，在视觉较敏感的区域嵌入少量秘密信息。位平面复杂度分割(Bit-Plane Complexity Segmentation, BPCS)[1]算法即是这样一种算法，它较好地利用了人类视觉对图像的冗余，在人类视觉不敏感的区域(位平面复杂度较高的块)嵌入秘密信息，隐藏容量大，隐蔽性好。BPCS算法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[2-3]。根据BPCS算法的原理还衍生出了一些新的隐藏方法[4]。但是BPCS算法在嵌入过程中会改变原始载体的复杂度的统计特性，留下了应用的安全隐患。本文分析了算法引起复杂度统计特性改变的原因，提出了一种改进的BPCS算法。实验证明，改进后的算法能有效抵抗针对BPCS复杂度统计特征的攻击。

2 BPCS隐藏算法和对BPCS算法的分析

BPCS隐藏算法是由LSB方法发展而来的。其主旨是将载体数据的多个位平面分成固定大小的小块，由于人的视觉对那些变化剧烈、复杂度高的位面小块不敏感，因此用这些位面小块来负载秘密信息[1]。这种方法顾及了人的视觉特性，有较高的隐蔽性；另外，秘密信息可以加载在多个位平面，所以它比LSB方法有更大的嵌入量。虽然BPCS算法有隐藏容量大、视觉隐蔽性好等优点，但是算法在嵌入秘密信息后会改变载体位面小块复杂度的统计特征，给隐写留下了安全漏洞。

设原始图像所有位平面小块的复杂度为 $h_O(c)$，秘密信息组成的位面小块的复杂度记为 $h_I(c)$，若用户选择的系统参数为 α，根据BPCS算法，对秘密信息小块的复杂度小于等于 $\alpha C_{\max}$ 的块作共轭处理($C_{\max}$ 是位面小块的最大复杂度)，则含密图像的位平面复杂度直方图为

$$h_S(c)=\begin{cases}h_O(c) & c\le \alpha C_{\max}\\ h_I(c) & \alpha C_{\max}<c<(1-\alpha)C_{\max}\\ h_I(c)+h_I(C_{\max}-c) & c\ge(1-\alpha)C_{\max}\end{cases} \quad (1)$$

由于被替换的小块数目与隐藏秘密信息的小块数目是相同的，因此

$$\sum_{c>\alpha C_{\max}} h_O(c)=\sum_{0\le c\le C_{\max}} h_I(c) \quad (2)$$

原始图像的直方图是对不同位平面许多小块进行统计的结果，所以连续性较好，从式(1)可以看出，含密图像复杂度直方图由3段组成，其直方图在段内光滑，而在段间衔接处会有剧烈的变化，且2个衔接处的横轴坐标关于 $0.5C_{\max}$ 对称。由式(1)可知，在 $(1-\alpha)C_{\max}$ 处，右侧高于左侧；又因为 $h_O(c)$ 集中于低端，所以在 $\alpha C_{\max}$ 处通常左侧高于右侧，可用不连续性测度 $d(c)$：

$$d(c)=[h(c-1)-h(c)]+[h(C_{\max}-c+1)-h(C_{\max}-c)],\ 0<c<0.5C_{\max} \quad (3)$$

来检测图像是否是含密图像，若 $d(c)$ 中存在明显的、大于0的峰值，则认为该图像含有秘密信息且秘密信息长度为

$$L=64\sum_{c\ge c_{peak}} h(c) \quad (4)$$

作者简介：娄振华(1983－)，男，硕士研究生，主研方向：信息隐藏；汤光明，教授

收稿日期：2007-11-28 **E-mail：**louzhenhua1983@sina.com

其中，c_{peak} 为 $d(c)$ 的峰值点，且 $c_{peak}=\lfloor \alpha C_{\max} \rfloor+1$（$\lfloor\ \rfloor$是向下取整）[5-6]。

3 改进的 BPCS 算法

不连续性测度在 c_{peak} 点处形成峰值，主要是因为含密图像的复杂度为 c_{peak} 的位面小块明显少于复杂度为 $\alpha C_{\max}$ 的位面小块；在其对应侧，复杂度为 $C_{\max}-c_{peak}$ 的位面小块明显少于复杂度为 $(1-\alpha)C_{\max}$ 的位面小块，所以在 $\alpha C_{\max}$ 处的前向差值和点 $(1-\alpha)C_{\max}$ 处的后向差值较大。若能在嵌入过程中相应地增加复杂度为 c_{peak} 和 $C_{\max}-c_{peak}$ 的位面小块数目比例，同时为了不致引出新的剧烈变化点，在 $(\alpha C_{\max},(1-\alpha)C_{\max})$ 范围内的复杂度位面小块的数目也应相应地增加，以保持其复杂度的变化趋势，确保不会产生新的不连续性测度峰值点，则不连续性测度就无法检测出图像载体是否经过 BPCS 隐藏消息了。基于此，提出了一种改进的 BPCS 算法。

首先将嵌入的消息划分为 2 部分，一部分是用户需要嵌入的秘密信息，另一部分则是一系列复杂度为 $\alpha C_{\max}<c<(1-\alpha)C_{\max}$ 的小块，用来调节由于嵌入秘密后复杂度直方图的不连续性，记这一调节部分的复杂度直方图为 $h_{adjust}(c)$，则含密图像复杂度直方图为

$$h_S(c)=\begin{cases}h_O(c) & c\le \alpha C_{\max}\\ h_I(c)+h_{adjust}(c) & \alpha C_{\max}<c<(1-\alpha)C_{\max}\\ h_I(c)+h_I(C_{\max}-c) & c\ge (1-\alpha)C_{\max}\end{cases} \tag{5}$$

由于图像中被替换位面小块数目与秘密信息和调节部分的小块数目之和是相同的，因此

$$\sum_{c>\alpha C_{\max}} h_O(c)=\sum_{0\le c\le C_{\max}} h_I(c)+\sum_{\alpha C_{\max}\le c\le(1-\alpha)C_{\max}} h_{adjust}(c) \tag{6}$$

从式(5)和式(6)可以看出，为了消除复杂度在 $\alpha C_{\max}\le c\le(1-\alpha)C_{\max}$ 范围内的剧烈变化，确保不会产生明显的不连续性测度峰值，关键是确定 $h_{adjust}(c)$ 的值（$\alpha C_{\max}<c<(1-\alpha)C_{\max}$）。

调节块中各复杂度块的数目 $h_{adjust}(c)$，$\alpha C_{\max}<c<(1-\alpha)C_{\max}$ 可通过以下算法确定：

首先确定用来调节复杂度直方图块的数目：

$$\sum_{\alpha C_{\max}\le c\le(1-\alpha)C_{\max}} h_{adjust}(c)=\beta\sum_{c>\alpha C_{\max}} h_O(c) \tag{7}$$

其中，β 是用户选择的参数；记 $p=\lfloor \alpha C_{\max} \rfloor$（$\lfloor\ \rfloor$是向下取整），令 $p'=C_{\max}-p$，计算

$$h_S'(c)=\begin{cases}h_O(c) & c\le \alpha C_{\max}\\ h_I(c) & \alpha C_{\max}<c<(1-\alpha)C_{\max}\\ h_I(c)+h_I(C_{\max}-c) & c\ge (1-\alpha)C_{\max}\end{cases} \tag{8}$$

其中，$h_S'(c)$ 是载体图像小于等于 $\alpha C_{\max}$ 的位面小块和秘密消息位面小块的复杂度统计。为了消除 $\alpha C_{\max}$ 处左侧高于右侧的剧烈变化，形成类似于原始图像复杂度直方图曲线在 $\alpha C_{\max}$ 处平缓变化的复杂度直方图，找出 $(p\ \ p')$ 内第 1 个大于 $h_S'(p)$ 的极大值点(若没有满足上述条件的点则找出 $(p\ \ p')$ 内的极大值点)，记该点为 q，计算

$$\Delta=(h_S'(q)-h_S'(p))/(q-p) \tag{9}$$

以 Δ 为 p 点和 q 点的之间的位面块的递增量，则

$$h_{adjust}'(c)=h_S'(p)+(i-p)\Delta-h_S'(c)\qquad p<c<q \tag{10}$$

同理，找出 $(p\ \ p')$ 内最后一个大于 $h_S'(p')$ 的极大值点(否则找出 $(p\ \ p')$ 内的极大值点)，记该点为 q'，则有

$$\Delta'=(h_S'(q')-h_S'(p'))/(q'-p') \tag{11}$$

$$h_{adjust}'(c)=h_S'(p')+(p'-i)\Delta'-h_S'(c)\quad q'<c<p' \tag{12}$$

将余下的调节块均匀地加在 $(p\ \ p')$ 内的直方图柱上，即

$$mean=(\beta\sum_{c>\alpha C_{\max}} h_O(c)-\sum_{\alpha C_{\max}\le c\le(1-\alpha)C_{\max}} h_{adjust}'(c))/(p'-p-1) \tag{13}$$

$$h_{adjust}(c)=h_{adjust}'(c)+mean\qquad p<c<p' \tag{14}$$

改进后的 BPCS 算法步骤如下：

(1)选择 α，β，计算图像中可用来嵌入秘密信息 M 的块和用来调节直方图块的总数。

(2)统计待嵌入消息的复杂度直方图，记为 $h_I(c)$。

(3)根据上面的算法确定调节直方图块部分中各复杂度的块数目 $h_{adjust}(c)$，$\alpha C_{\max}<c<(1-\alpha)C_{\max}$。

(4)从预先建立的复杂度位面库中取出相同数目的复杂度块，将各块顺序置乱后附加在秘密消息块后组成新的待嵌入消息 M'。

(5)将 M' 替换载体图像中位平面复杂度大于 $\alpha C_{\max}$ 的块，M' 中复杂度小于等于 $\alpha C_{\max}$ 要经共轭处理。

(6)记录下来哪些小块是经过共轭处理的，将这部分信息连同系统参数 α，β 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。

接收方接收消息的过程同样简单，先将所有复杂度大于 $\alpha C_{\max}$ 的块取出，取出块总数的前 $(1-\beta)100\%$ 为秘密消息，其中经过共轭处理的块可同样由额外的信息标记并经共轭处理后得出。

系统参数 α 取值与原 BPCS 算法要求一样，系统参数 β 越大，可供用户调节复杂度直方图的块的数目越多，则可使得含密图像的复杂度直方图更接近原始图像的复杂度直方图，但是 β 越大可供用户嵌入的有效秘密信息也越少；反之，β 越小，虽然有效嵌入秘密信息越多，但可供用户调节复杂度直方图的块的数目越少，含密图像复杂度直方图就易剧烈变化。一般来说，β 取值为[0.15, 0.3]之间可较好地协调算法安全性与有效嵌入量之间的关系。

4 实验结果

为验证改进算法的有效性，在大小为 512×512 的标准灰度图像Lena[7]上分别使用文献[1]提出的BPCS算法和本文改进后的BPCS算法嵌入秘密信息。当 $\alpha=0.43$ 时，BPCS算法嵌入的秘密信息量为 5.2×10^5 bit，隐藏信息引起的PSNR为37.1 dB，使用改进的BPCS算法嵌入秘密信息时选择 $\beta=0.2$ 时，嵌入 5.2×10^5 bit信息，隐藏信息引起的PSNR为 37.2 dB，有效秘密信息量为 4.17×10^5 bit。不连续性测度的结果如图 1~图 3 所示。

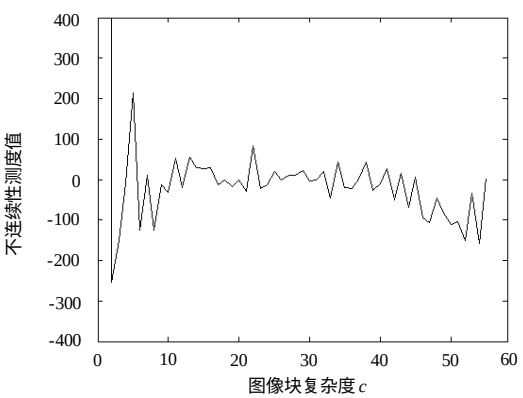

图 1　原始图像复杂度不连续性测度

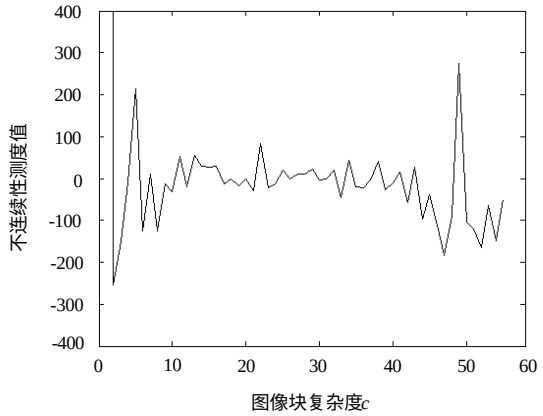

图 2　BPCS 嵌入秘密信息后的不连续性测度

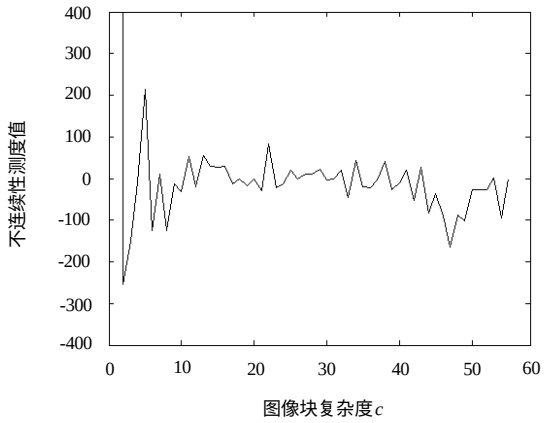

图 3　改进算法嵌入后的不连续性测度

在图 2 中，BPCS 嵌入信息后，在复杂度为 49($\alpha C_{\max} = 0.43\times112 = 48.16$)处不连续测度 $d(c)$ 有一处明显的峰值，显示是经过 BPCS 隐藏过的图像。

而在图 3 中，与标准 lena 图像复杂度不连续性测度(图 1)类似，几乎没有明显的不连续性测度峰值，当然也就不能判断图像是否为含密图像了。由于 BPCS 算法的嵌入容量较大，改进后的算法在 $\alpha = 0.43$ 时虽然牺牲了 20%的容量，但是仍然能达到 1.59 bit/像素，保持了 BPCS 算法嵌入容量大的优点。

下面给出另外 3 幅标准灰度测试图像(512×512)Peppers, Tank, Boat[7]进行相同实验的结果，如图 4~图 6 所示，实验以峰值信噪比(Peak Signal to Noise Ration, PSNR)作为图像质量评价的客观标准，使用伪随机序列作为秘密信息，位面小块尺寸取 8×8，β 取 0.2，α 取 0.43。实验结果如表 1 所示。

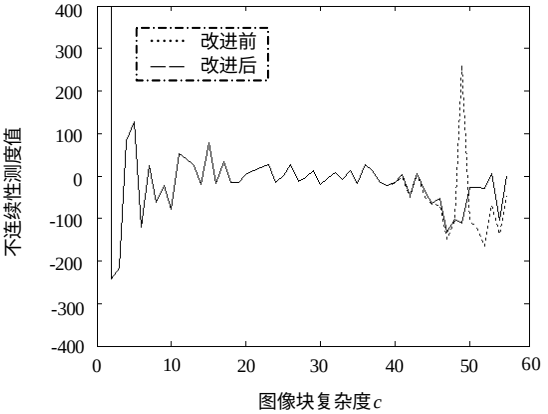

图 4　Peppers 在改进算法前后的不连续性测度比较

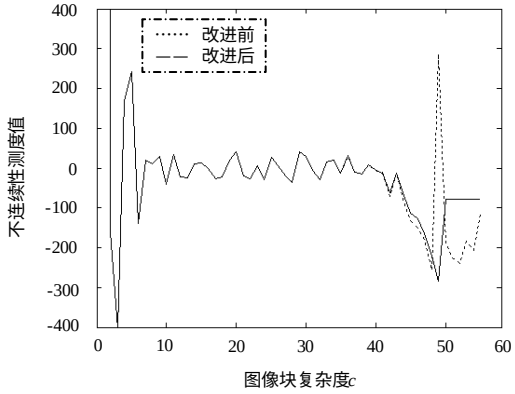

图 5　Tank 在改进算法前后的不连续性测度比较

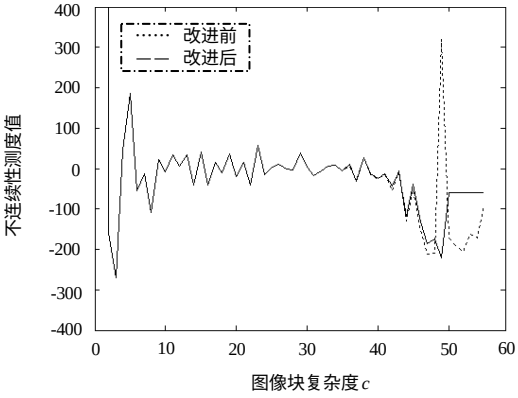

图 6　Boat 在改进算法前后的不连续性测度比较

表 1　测试图像性能比较

性能($\alpha = 0.43$, $\beta = 0.2$)		嵌入量/bit		性噪比/dB	
		原 BPCS 算法	改进后算法	原 BPCS 算法	改进后算法
图像	Peppers	515 648	412 544	38.3	38.3
	Tank	875 072	700 032	31.9	32.0
	Boat	773 824	619 072	32.9	32.8

实验结果证明了改进后的 BPCS 算法能较好地抵抗针对 BPCS 的统计分析，也保持了原 BPCS 算法大容量的特点。

5　结束语

BPCS 算法隐藏信息后，在其复杂度直方图上留下了 2 点明显的不连续性，检测者据此能检测到图像载体是否经过 BPCS 隐藏信息，成为其安全漏洞。本文提出的改进后的 BPCS 算法能有效克服这一弱点，使得嵌入信息后的复杂度仍然连续，从而使针对 BPCS 复杂度直方图统计特征的检测算法失效，在保持嵌入容量大的特点上有效地提高了算法的安全性。

参考文献

[1] Kawaguchi E, Eason R O. Principle and Application of BPCS-steganography[C]//Proc. of SPIE International Symposium on Voice, Video, and Data Communications: Multimedia Systems and Applications. Boston, MA, USA: [s. n.], 1998: 464-472.

[2] Spaulding J, Shirazi M N, Kawaguchi E, et al. Application of Bit-plane Decomposition Steganography to JPEG2000 Encoded Images[J]. IEEE Signal Processing Letters, 2002, 9(12): 410-413.

[3] Spulding J, Noda H, Shirazi M N, et al. BPCS Steganography Using EZW Lossy Compressing Images[J]. Pattern Recognition Letters, 2002, 23(13): 1579-1587.

（下转第 205 页）