第17卷 第7期 计算机辅助设计与图形学学报 Vol.17, No.7
2005年7月 JOURNAL OF COMPUTER-AIDED DESIGN & COMPUTER GRAPHICS July, 2005

对空域BPCS密写的统计分析

张新鹏 王朔中
(上海大学通信与信息工程学院 上海 200072)
(zhangxinpeng@263.net)

摘 要 位面复杂度分割(BPCS)密写法将复杂度较高的位平面小块用秘密信息替换,可以嵌入较多的秘密信息并维持较好的隐蔽性,但含密图像的位平面小块复杂度直方图中存在两个明显的不连续点.据此,提出了针对BPCS密写的分析方法,由复杂度直方图的不连续性可以判断秘密信息的存在性,并确定秘密信息块的复杂度范围,准确测算秘密信息嵌入量.这种分析方法的原理同样适用于变换域位面复杂度分割密写.

关键词 信息隐藏;密写分析;位面复杂度分割;直方图
中图法分类号 TP911.73

Statistical Analysis Against Spatial BPCS Steganography

Zhang Xinpeng Wang Shuozhong
(*School of Communication and Information Engineering, Shanghai University, Shanghai* 200072)

Abstract Bit-plane complexity segmentation (BPCS) steganography replaces bit-plane blocks of high complexity with secret data, providing large embedding capacity and good imperceptibility. By constructing a histogram of bit-plane block complexity, however, a security flaw in the BPCS method is revealed. Two striking discontinuities in the complexity histogram unambiguously announce the presence of BPCS-based hidden information. Furthermore, the complexity criterion used in data embedding can be estimated quite accurately, leading to a good estimation of the embedding capacity. The steganalytic technique proposed in this paper is equally effective against BPCS steganogrphy both in the spatial (temporal) domain and in the transform domain.

Key words information hiding; steganalysis; BPCS (Bit-Plane Complexity Segmentation); histogram

1 引 言

密写是信息隐藏的一个重要分支[1],其目的是将信息秘密、安全地发送出去而不引起第三方的怀疑.作为密写的对抗技术,密写分析的目的则是检测多媒体载体中敌对秘密信息的存在性,它所面对的是数量巨大的可疑对象以及复杂多变的密写技术.因此,目前对密写分析的研究主要是针对特定密写技术的.如果在不知密钥的情况下能够对已有的主要密写技术分别实施成功的分析,就能挫败大量的敌对密写行为.预计在相当长一段时间里,这仍将是密写分析研究的主流.迄今为止,已出现了针对不同载体类型、不同密写算法的多种分析方法[2-3].在实际应用中,并不要求分析者提取出具体的传送内容,只要能够确认载体数据中含有秘密信息,密写分析即告成功,信道监控者可以藉此中止密写方和接收方的通信或追查秘密信息来源.

收稿日期:2004-02-10;**修回日期**:2004-04-12
基金项目:国家自然科学基金(60372090);上海市科委基础研究重点项目(04JC14037)

最低比特位(Least Significant Bit, LSB)密写法是出现较早的一种时/空域密写技术[4]. 其实现比较容易,隐藏时用秘密信息直接替换载体数据最不重要的比特位,提取秘密信息时将最低比特位取出即可. 目前已有几种分析方法可以有效攻击 LSB 密写,包括利用各图像块的正则性和奇异性的 RS (Regular Singular)方法[5]、利用载体数据直方图特性的 χ^2 统计法[6]、利用相邻像素穿越不同平面簇频率的 GPC(Gray-Level Plane Crossing)方法[7]等. 对 LSB 方法进行合理的改进可以使安全性大大提高,有效抵抗这些分析方法[8-9].

位平面复杂度分割(Bit-Plane Complexity Segmentation, BPCS)密写是 LSB 方法的发展,性能优于简单的 LSB 方法. 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,所以用这些位面小块来负载秘密信息[10]. 这种方法顾及了人的视觉特性,因此有较好的隐蔽性;另外,秘密信息可以加载在多个位平面,所以比 LSB 方法有更大的嵌入量. 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[11-12],根据 BPCS 密写的原理还衍生出了一些新的密写方法[13]. 本文设计了针对空域 BPCS 的密写分析法,应用这种方法不但能检测出秘密信息的存在性,而且可以准确地估计秘密信息嵌入量,这种分析法也可推广到变换域 BPCS 密写.

2 BPCS 密写

无论应用于时空域还是应用于小波压缩域,BPCS 的原理和嵌入方法都是相同的,仅仅是位平面的意义有所区别,下面主要考虑将 BPCS 方法应用于静止图像空间域的情况.

BPCS 密写方法如下:

Step1. 先将载体图像的所有位平面分成相同大小的小块,如 8×8.

Step2. 计算每个小块的复杂度,其定义为所有相邻像素对中取值不同(即一个为 0,另一个为 1)的像素对数目. 复杂度的最大可能值记为 C_{max}. 如果位面小块的大小为 8×8,那么复杂度的取值范围就是 0 和 112 之间的整数. 当位平面小块为全 0 或全 1 时,复杂度取为最小值 0;而当位平面小块为如图 1 所示棋盘状时,复杂度取为最大值 C_{max},即 112.

Step3. 将复杂度大于 $\alpha\cdot C_{max}$ 的位面小块用于负载秘密信息,这里 α 是系统参数,其值要小于 0.5,例如取 $\alpha=0.4$, α 取得越小可以嵌入的秘密信息量就越多.

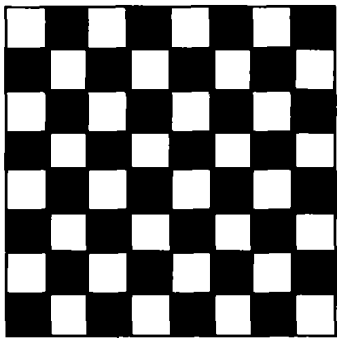


图 1 棋盘状小块:白格代表 1;黑格代表 0

Step4. 由秘密信息组成位面小块,如果其复杂度大于 $\alpha\cdot C_{max}$,直接替换原位面小块;否则要作共轭处理,就是将秘密信息组成的位面小块与棋盘状小块作异或生成新的小块. 设共轭处理前的复杂度为 c,那么共轭处理后的复杂度必为 $C_{max}-c$. 因为 $\alpha<0.5$,所以新小块的复杂度一定大于 $\alpha\cdot C_{max}$. 共轭处理后,用新的小块替换原始数据的位面小块.

Step5. 记录下来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. 例如可以用 LSB 方法或量化索引调制方法(Quantization Index Modulation, QIM)方法[14]将这些额外的信息隐藏在预先划定的区域.

接收方的提取过程很简单:将载体数据中所有复杂度大于 $\alpha\cdot C_{max}$ 的位面小块取出;再提取出 Step5 中额外嵌入的信息,确定哪些小块经过了共轭处理. 将经过共轭处理的小块与棋盘状小块作异或便可恢复出秘密信息.

在静止图像的空间域应用 BPCS 方法时往往不采用二进制形式划分位平面,而是采用循环码划分位平面. 设一个数字的二进制形式为 $(B_{N-1}B_{N-2}\cdots B_1B_0)$,循环码形式为 $(G_{N-1}G_{N-2}\cdots G_1G_0)$,它们可以按照如下规则互相转换

$$G_{N-1}=B_{N-1},G_{N-2}=B_{N-1}\otimes B_{N-2},$$
$$G_{N-3}=B_{N-2}\otimes B_{N-3},\cdots,G_0=B_1\otimes B_0;$$
$$B_{N-1}=G_{N-1},B_{N-2}=B_{N-1}\otimes G_{N-2},$$
$$B_{N-3}=B_{N-2}\otimes G_{N-3},\cdots,B_0=B_1\otimes G_0.$$

其中,符号$\otimes$表示异或运算. 表 1 给出了数字 0~7 的二进制码和循环码. 如果用二进制形式划分位平面,会有许多小块的复杂度大于 $0.5C_{max}$,而 BPCS 密写又要求 $\alpha<0.5$,所以密写会引起较大的失真. 而应用循环码划分位平面可以使绝大多数小块的复杂度在 $0.5C_{max}$ 以下,因而可方便地设置 α 值来调节信息的隐蔽性和嵌入量.

表 1　数字 0～7 的二进制码和循环码

十进制	二进制	循环码
0	000	000
1	001	001
2	010	011
3	011	010
4	100	110
5	101	111
6	110	110
7	111	100

3　BPCS 密写分析

首先讨论 BPCS 密写行为. 我们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 $h_O(c)$,$(0 \leqslant c \leqslant C_{max})$. 由于图像相邻像素之间具有较强的相关性,而且位平面越高相邻比特之间的相关性就越强,故 $h_O(c)$ 通常集中于 c 值较低的一侧. 又因为 $h_O(c)$ 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. 图 2 所示为根据 512×512 的标准灰度图像 Man 按 8×8 分块得到的复杂度直方图. 由于高位面相关性很强,有大量复杂度为 0 的块,同时又因为复杂度不可能为 1,所以在 c 值接近于 0 处起伏剧烈,不在考虑范围之内.

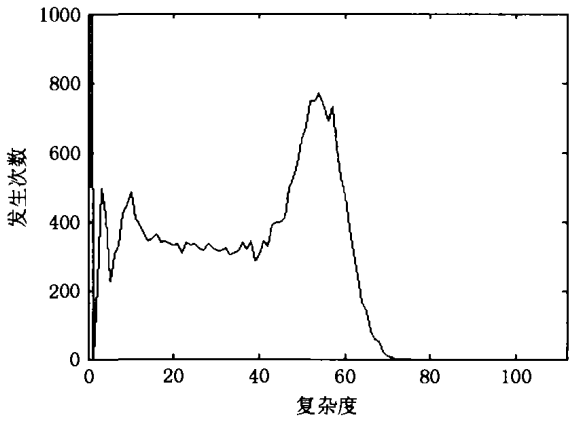


图 2　由原始图像 Man 得到的复杂度直方图

BPCS 密写将复杂度大于 $\alpha \cdot C_{max}$ 的位面小块取出,置换为秘密信息组成的小块. 秘密信息通常都经过加密或压缩处理,基本没有信息冗余,可以认为类似于随机信号. 一个 8×8 的小块含有 112 个相邻像素对,每一像素对中两个像素取值不同的概率为 0.5,而复杂度就是小块中取值不同的像素对总数,这种情况与中心极限定理的条件相似[10],故秘密信息小块的复杂度近似于正态分布. 图 3 所示为由10 000个秘密信息小块得到的复杂度直方图,文献[10]对4 096 000个秘密信息小块进行了统计,其结果很好地符合正态分布:均值为 $0.5C_{max}$,标准差为 $0.047C_{max}$.

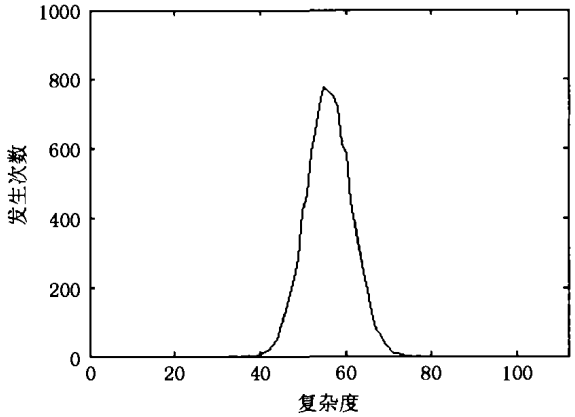


图 3　由 10^4 个秘密信息小块得到的复杂度直方图

将秘密信息组成的位面小块的复杂度直方图记为 $h_I(c)$,当秘密信息小块的复杂度小于等于 $\alpha \cdot C_{max}$ 时要作共轭处理,所以密写图像的位面小块复杂度直方图

$$h_S(c) = \begin{cases} h_O(c), & c \leqslant \alpha \cdot C_{max} \\ h_I(c), & \alpha \cdot C_{max} < c < (1-\alpha) \cdot C_{max} \\ h_I(c) + h_I(C_{max} - c), & c \geqslant (1-\alpha) \cdot C_{max} \end{cases} \tag{1}$$

这里,因为被替换的小块数目与隐藏秘密信息的小块数目是相同的,所以

$$\sum_{c > \alpha \cdot C_{max}} h_O(c) = \sum_{0 \leqslant c \leqslant C_{max}} h_I(c).$$

从式(1)可以看出密写后的复杂度直方图 $h_S(c)$ 由三段组成,每一段都是比较光滑的,但在不同段之间的衔接处则会有剧烈的变化. 而且,这两个衔接处的横轴坐标和恰为 C_{max},即关于 $0.5C_{max}$ 对称. 由式(1)可知在 $(1-\alpha) \cdot C_{max}$ 处,右侧高于左侧;又因为 $h_O(c)$ 集中于低端,所以在 $\alpha \cdot C_{max}$ 处通常左侧高于右侧.

经过以上分析,我们给出如下的密写分析方法:

将待检测图像各位平面划分为小块,统计复杂度直方图为 $h(c)$,计算不连续性测度

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

这里所定义的 $d(c)$ 是 $h(c)$ 在 c 处的逆向差分与 $(C_{max} - c)$ 处正向差分的总和,可以用来衡量 $h(c)$ 的不连续性. 如果 $d(c)$ 中存在明显的、大于 0 的峰值则可以认为该图像含有秘密信息. $d(c)$ 在其最大值处是否为峰值,可用 $d(c)$ 中最大值与次大值的比值是否大于某一阈值 T(例如 $T = 2.5$)来判断. 如果 $d(c)$ 中的峰值处于点 c_{peak} 处,则说明复杂度在 c_{peak} 以上的小块被用来负载秘密信息,所以秘密信息长度为

$$L = 64 \cdot \sum_{c \geqslant c_{peak}} h(c) \qquad (2)$$

4 实验结果

由图 2 所示的标准灰度图像 Man 的直方图得到的 $d(c)$如图 4 所示,可见在 c 值距 0 较远的地方没有明显的峰值. 以 Man 作为原始载体进行 BPCS 密写,位面小块尺寸取为 8×8,当 $\alpha=0.4$ 时,嵌入量为 7.2×10^5 bit,密写引起的 $PSNR=33.5$ dB. 实施本文提出的密写分析方法,得到的复杂度直方图与 $d(c)$如图 5 所示. 在 $c=45$ 处存在一个明显的峰值,可知复杂度大于等于 45 的位面小块被用于负载秘密信息,统计这样的小块的个数为 1.1×10^4,再根据式(2)乘以 64 便可准确得到秘密信息的长度. 类似地,当 $\alpha=0.45$ 时嵌入量为 5.2×10^5 bit,密写引起的 $PSNR=36.7$ dB,密写分析得到的复杂度直方图与 $d(c)$如图 6 所示,峰值处于 $c=51$ 处,根据式(2)同样可以计算秘密信息的长度,与实验中嵌入的比特数相符.

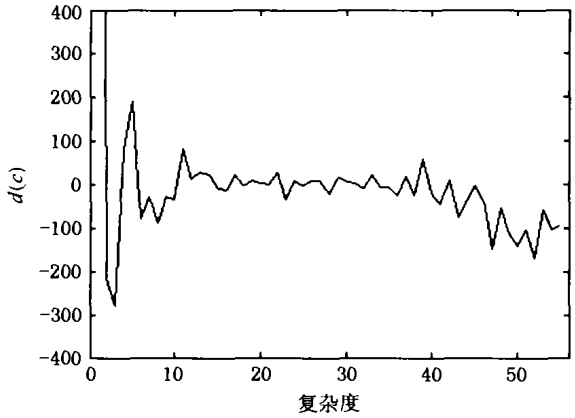
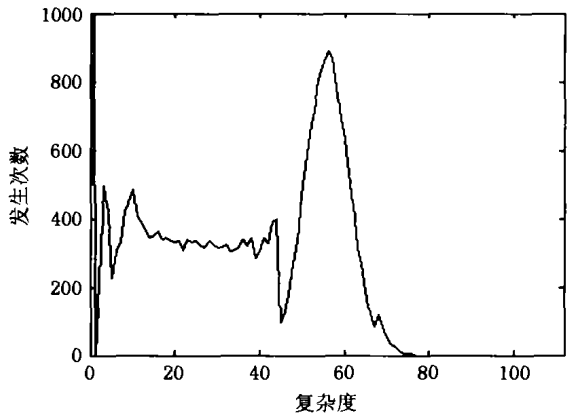
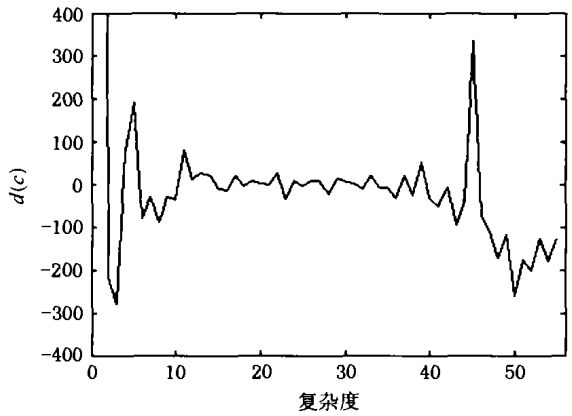


图 4 原始图像复杂度直方图的不连续性测度 $d(c)$

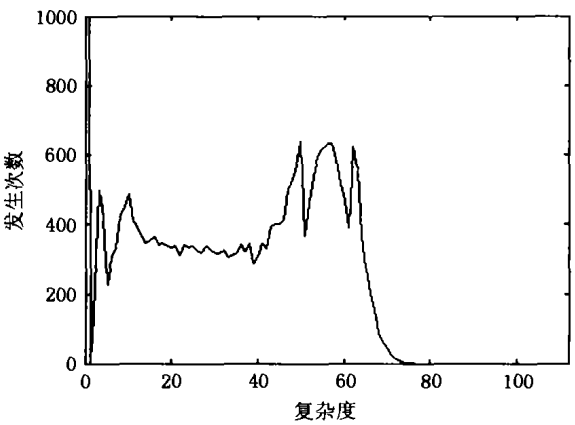


a 复杂度直方图 $h(c)$

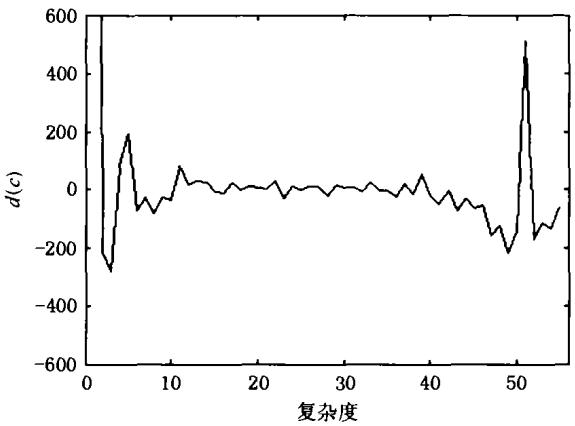


b 不连续性测度 $d(c)$

图 5 $\alpha=0.4$ 时的密写分析



a 复杂度直方图 $h(c)$



b 不连续性测度 $d(c)$

图 6 $\alpha=0.45$ 时的密写分析

对多幅图像 Lena,Baboon,Bridge,Lake,Peppers 等进行测试,本文方法均可以有效检测出秘密信息的存在性,并准确测算秘密信息嵌入量. 用数字照相机获取一百余幅灰度图像,内含人物及风景,大小为 300×400,以这些图像为载体并以不同的 α 分别进行密写(即嵌入量不同),然后用本文方法进行分

析. 在 Pentium1.7 GHz,512 MB 内存、Matlab 环境下分析每幅图像平均用时 9 s. 表 2 给出了分析结果,即不同嵌入量时,选取不同阈值 T 时的两类错误概率.虚警表示将原始载体误认为含有秘密信息,漏检表示将密写图像误作原始图像. 从表 2 可以看出,阈值 T 增大时,虚警概率变小而漏检概率变大;阈值 T 减小时,虚警概率变大而漏检概率变小. 如果我们要求漏检概率较小,而对虚警的要求不是很严格,那么可以选择较小的阈值. 综合两种错误概率,我们推荐阈值取为 2.50. 一般说来,较大的秘密信息量会损害载体图像的质量,密写者会尽量避免这种情况. 而当秘密信息量较小时(即 α 接近 0.5),$d(c)$中的峰值也很明显,应用本文方法依然有效,即在 α 接近 0.5 时有较小的漏检概率(如表 2 所示). 一旦检测出载体中存在秘密信息,便可以根据复杂度直方图中峰值的位置准确地估计嵌入量.

表 2　不同阈值时的检测性能　　%

T	虚警概率	漏检概率			
		$\alpha=0.40$	$\alpha=0.425$	$\alpha=0.45$	$\alpha=0.475$
2.0	5.04	1.68	0.84	0	0
2.5	1.68	4.20	3.36	0	0.84
3.0	0.84	7.56	5.88	3.36	2.52

5　结　　论

尽管 BPCS 密写应用视觉特性可以保证较好的隐蔽性,但在位面小块复杂度直方图中出现了两个明显的不连续点,成为其安全漏洞. 由此可定义一个复杂度直方图的不连续性测度 $d(c)$,用以分析秘密信息的存在性. 根据 $d(c)$还可以进一步确定 BPCS 嵌入算法中所用的 α 值,从而准确计算出秘密信息的长度.

虽然 BPCS 密写可以在空间域和小波域有不同应用,但其原理和基本方法是相同的,仅仅是位面的意义有所不同,因此本文提出的密写分析方法可以推广到变换域 BPCS 密写.

参　考　文　献

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

[2] Wang H, Wang S. Cyber warfare-steganography vs. steganalysis [J]. Communications of the ACM, 2004, 47(10): 76～82

[3] Fridrich J, Goljan M. Practical steganalysis of digital images-state of the art [A]. In: Security and Watermarking of Multimedia Contents IV, Proceedings of SPIE 4675 [C]. San Jose, 2002. 1～13

[4] Bender W, Gruhl D, Morimoto N, *et al*. Techniques for data hiding [J]. IBM System Journal, 1996, 35(3,4): 313～336

[5] Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and gray-scale images [J]. Magazine of IEEE Multimedia, Special Issue on Security, 2001, 8(4): 22～28

[6] Westfeld A, Pfitzmann A. Attacks on steganographic systems [A]. In: The 3rd International Workshop on Information Hiding, Lecture Notes in Computer Science 1768 [C]. Dresden: Springer-Verlag, 1999. 61～76

[7] Zhang Xinpeng, Wang Shuozhong, Zhang Kaiwen. Steganalysis based on the statistics for LSB insertion [J]. Journal of Applied Sciences, 2004, 22(1): 16～19 (in Chinese)
(张新鹏, 王朔中, 张开文. 基于统计特性的 LSB 密写分析 [J]. 应用科学学报, 2004, 22(1): 16～19)

[8] Zhang Xinpeng, Wang Shuozhong, Zhang Kaiwen. A novel LSB steganography scheme against statistical analysis [J]. Journal of Image and Graphics, 2003, 8A(9): 1055～1060 (in Chinese)
(张新鹏, 王朔中, 张开文. 抗统计分析的 LSB 密写方案[J]. 中国图象图形学报, 2003, 8A(9): 1055～1060)

[9] Zhang Xinpeng, Wang Shuozhong, Zhang Kaiwen. Steganography with least histogram abnormality [A]. In: Computer Network Security, Lecture Notes in Computer Science 2776 [C]. St, Petersburg: Springer-Verlag, 2003. 395～406

[10] Kawaguchi E, Eason R O. Principle and application of BPCS-steganography [A]. In: Multimedia Systems and Applications, Proceedings of SPIE 3528, Boston, 1998. 464～472

[11] Noda H, Spaulding J, Shirazi M N, *et al*. Application of bit-plane decomposition steganography to JPEG2000 encoded images [J]. IEEE Signal Processing Letters, 2002, 9(12): 410～413

[12] 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

[13] Hioki H. A data embedding method using BPCS principle with new complexity measures [OL]. http://www.know.comp.kyutech.ac.jp/STEG02/Papers/pdf-files/O05-Hioki.pdf

[14] Chen B, Wornell G W. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding [J]. IEEE Transactions on Information Theory, 2001, 47(4): 1423～1443

张新鹏　男,1975 年生,博士,讲师,主要研究方向为数字水印、密写与密写分析、数字图像处理、ATM 交换等.

王朔中　男,1943 年生,博士,教授,博士生导师,主要研究方向为图像处理、音频信号处理、信息隐藏.