基于图像分类的矢量量化数字水印算法。

顾 伟, 吕皖丽, 罗 斌 (安徽大学 计算机科学与技术学院, 合肥 230039)

摘 要:通过提取熵和标准差两个特征对图像进行分类,将分类结果采用 PNN 算法进行矢量量化,将其生成的码书作为 LBG 算法的初始码书以降低该算法对初始码书敏感的缺点。同时在水印提取过程中,首先对码书进 行预处理以减少图像攻击对码书的影响,再提取水印图像。实验证明,使用该方法不仅得到了较高的图像质量, 而且对常见的攻击也具有鲁棒性。另外,在传输过程中对码书和索引值的窜改,也具有一定的抗攻击性。 关键词: 矢量量化;码书;图像分类;数字水印

中图分类号: TP391.7;TP309 文献标志码: A 文章编号: 1001-3695(2009)07-2738-03 doi:10.3969/j.issn.1001-3695.2009.07.097

Digital watermark algorithm of vector quantization based on image classification

GU Wei, LV Wan-li, LUO Bin

(School of Computer Science & Technology, Anhui University, Hefei 230039, China)

Abstract: Image region is classified by the entropy and the standard deviation, and then quantized by PNN algorithm separately. Additionally, used the codebook generated by PNN algorithm to the initial codebook of LBG algorithm for reducing LBG algorithm's sensitivity. Particularly, in watermark extracting process, preprocessed the codebook to decrease influence on co-debook. Experimental results show that the proposed algorithm not only improves codebook quality evidently, but also is robust to common image processing operations. In addition, the proposed algorithm has some anti-attack capability for tampering with codebook and index values.

Key words: vector quantization; codebook; image classification; digital watermark

0 引言

互联网的普及为多媒体信息的存取提供了极大的便利,提 高了信息表达的效率和准确性。如何保护多媒体数据的安全, 即行之有效的版权保护成为重要的研究课题。数字水印技术 作为信息隐藏和版权保护的一种手段,在图像、声音、文档、视 频等多种数字化的产品中得到了广泛的应用,成为多媒体信息 安全研究领域的一个热点问题。

由于矢量量化(vector quantization, VQ)具有压缩率高、解码简单和易于硬件实现的优点^[1],近年来已广泛地应用于图像、语音信号的处理中。出现了多种基于矢量量化技术的数字水印算法^[2-4]。

码书设计是矢量量化的关键问题之一。传统的 LBG 算法^[5]存在一些较为明显的缺点,如对初始码书依赖性较高,容易 陷入局部最优的缺点^[6]。因此,有不少学者提出了改进方法,如 最大下降法(maximum descent, MD)^[7]、基于神经网络的矢量量 化码书设计算法^[8]、基于遗传算法的码书设计算法^[9]等。

本文针对矢量量化过程中码书设计存在的问题提出自己 的改进。将图像分类的方法应用于码书设计中,提出了一种改 进的基于图像分割的矢量量化盲水印算法。同时,为了使嵌入 的水印能够抵抗图像攻击和对码书、索引值的窜改,在提取水 印过程中,对码书进行预处理。

1 基于图像分类的码书设计

设计性能良好的码书是矢量量化的关键。码书设计最基本的算法是 1980 年 Linde 等人^[5]提出了 LBG 算法。其基本思想是随机选择一个初始码书,按最近邻原则对所有训练矢量确定一个划分,计算由这种划分所带来的量化失真;再根据质心原则产生新的码书,然后根据新码书再次对训练矢量进行划分,不断重复此过程,直至量化失真下降的比率小于设定的阈值为止。传统的 LBG 算法虽然算法简单、易于实现,但是存在着对初始码书敏感、不易得到全局最优码书的缺点。同时,传统的 LBG 算法对图像进行矢量量化时,将图像子块看成互不相关的部分,忽略了图像本身的相关性和冗余性。

本文为了提高码书的质量,一方面针对 LBG 算法对初始 值敏感的缺点,引入成对最近邻(pairwise nearest neighbor, PNN)算法^[10],将其结果作为 LBG 算法的初始码书,使其能够 较好地在整个训练矢量空间中散开,较好地反映训练矢量的整 体分布特征;另一方面,将图像分类的思想应用于矢量量化中, 通过提取每个图像子块熵和标准差两个特征,将图像划分为光

收稿日期: 2008-10-22; 修回日期: 2008-12-27 基金项目: 国家自然科学基金资助项目(60772122);博士点基金资助项目(20070357001)

作者简介:顾伟(1982-),男,安徽合肥人,硕士,研究方向为模式识别与图像处理、数字水印等(maths2007@163.com);吕皖丽(1974-),女,安徽合肥人,博士,研究方向为模式识别与图像处理、数字水印;罗斌,男,安徽合肥人,教授,博导,研究方向为模式识别与图像处理.

滑区、一般区和纹理区三个区域,然后分别对这三个区域量化 编码,生成码书。分类方法如图1所示。



图像的熵是一种特征的统计形式,它反映了图像中平均信息量的多少。文献[11]中通过计算图像的熵和标准差将图像分为光滑区、纹理区、边缘区和一般区,并研究指出图像光滑区域的熵和标准差都较小;纹理区域的熵值较大,标准差较小;边缘区域的熵和标准差都较大。

对矢量量化而言,图像分类数越多反而有可能造成图像质量的下降^[12]。故本文为了获得较好的图像质量,仅将图像划分为光滑区、一般区、纹理区三个区域。图1中*En*1、*En*2、*Std*1、*Std*2均为分割阈值。在这里,按照文献[11]的方法取分割阈值*En*1=1.8,*En*2=2.5,*Std*1=20,*Std*2=40。

设训练矢量集为 $X = \{x_0, x_1, \dots, x_{M-1}\}$,待生成的码书为 $C = \{c_0, c_1, \dots, c_{N-1}\}$ 。其中训练矢量 $x_i = \{x_{i0}, x_{i1}, \dots, x_{i(k-1)}\}$ $(0 \le i \le M - 1)$,码书中的码字 $c_j = \{c_{j0}, c_{j1}, \dots, c_{j(k-1)}\}$ $(0 \le j \le N - 1)$, k 是矢量的维数。具体步骤如下:

a) 将大小为 $W \times H$ 原始图像 HI 划分为互不重复的大小 为 $n \times n$ 子块,再将每个子块转换为 $1 \times k(k = n \times n)$ 的训练矢 量,则产生 $M = \lfloor W/n \rfloor \times \lfloor H/n \rfloor$ 个训练矢量,即 $X = \{x_0, x_1, \dots, x_{M-1}\}$ 。这里取 n = 4。

b)分别依据式(1)和(2)计算每一图像子块的特征值:摘 En和标准差 Std。根据特征值的大小将相应的训练矢量划分 为光滑区 T₁、纹理区 T₂和一般区 T₃。

$$En = -\sum_{i=1}^{k} P(i) \log_2 P(i)$$
(1)

$$Std = \sqrt{1/n^2 \sum_{i=1}^{n} \sum_{j=1}^{n} f^2(i,j) - (1/n^2 \sum_{i=1}^{n} \sum_{j=1}^{n} f(i,j))^2}$$
(2)

c)确定不同区域的码书大小N_i。不同区域码书的大小由 该区域包含的训练矢量个数占全部训练矢量个数的比例来决 定。对每个区域分别执行 d) e)。

d) 对区域 T_i (*i*=1,2,3) 执行 PNN 算法,生成码书 C_i^0 。

e)将 C_i^0 作为初始码书,再执行LBG算法,生成码书 C_i 。

f)合并码书 C_i (*i*=1,2,3),生成大小为 *N* 的码书 $C = \{c_0, c_1, \dots, c_{N-1}\}_{\circ}$

2 水印嵌入过程

设原始图像 HI 大小为 W×H,水印图像 WI 大小为 w×h。 水印嵌入过程如图 2 所示,详细步骤如下:

a) 将原始图像 *HI* 转换为训练矢量集 *X* = {*x*₀, *x*₁, …, *x*_{*M*-1}},将水印图像 *WI* 进行 Arnold 变换并转换成大小为 1 × $k'(k' = w \times h)$ 的矢量 *wm* = { ω_{00} ,……, $\omega_{0(h-1)}$, ω_{10} ,…, $\omega_{1(h-1)}$, …, $\omega_{(w-1)(h-1)}$ }。

b) 根据码书生成步骤生成原始图像 *HI* 的码书 $C = \{c_0, c_1, \dots, c_{N-1}\}_{\circ}$

c) 将码书 C 划分为大小相等的子码书 P⁰ 和 P¹, 使子码

书中位置相同的码字 $P_j^0 \in P^0$ 和 $P_j^1 \in P^1$ 在码书中的距离最小。 其中 $P^i = \{p_0^i, p_1^i, \dots, p_{(N2)-1}^i\}, i = \{1, 2\}$ 。

d) 依次输入训练矢量 x_i ($0 \le i \le M - 1$) 和水印值 ω_{xy} ($0 \le x \le w, 0 \le y \le h$),在码书 C 中查找与 x_i 距离最近的码字 c_p ($0 \le p \le N - 1$),如果 $\omega_{xy} = 0$ 且 $c_p \notin P^0$,则用 $c'_p \in P^0$ 代替;若 $\omega_{xy} = 1$ 且 $c_p \notin P^1$,则用 $c'_p \in P^1$ 代替。其中 c_p 和 c'_p 是两个子码 书中距离最近的码字。最后记录输入训练矢量 x_i 与相应码字 c_j 之间对应关系。

e) 重复执行 d),直至所有的水印值 $\omega_{xy}(0 \le x \le w, 0 \le y \le h)$ 嵌入完毕,同时生成记录训练矢量 x_i 与对应码字 c_j 之间 关系的索引表 table。

至此,水印的嵌入完成。如需重建图像和提取水印,则只 要将码书和索引表传递给接收端即可,无须原始图像参与,因 此水印的提取属于盲水印提取。

3 水印的提取过程

为了抵抗在传输过程中,码书受到的有意或无意的干扰和 攻击,在提取水印之前,需要对码书进行预处理。基本思想是 首先检查码书中的码字是否存在异常值,若存在,则找出这些 异常值在图像中的对应位置,利用图像自身的相关性,使用异 常值在图像中对应位置的相邻像素点的均值代替码字中异常 值。水印提取的具体过程如下:

a)检查码书 C 中码字的取值范围是否在合理的范围之内。如果是,则转向 b);否则,则将码字中不合理的值用相邻 像素点的均值代替。

b) 将码书 C 按相同的方法划分为大小相等的子码书 P^{0} 和 P^{1} 。其中: $P^{i} = \{p_{0}^{i}, p_{1}^{i}, \dots, p_{(N2)-1}^{i}\}, i = \{1, 2\}$ 。

c)如仅需重建原始图像,转d);若仅需提取水印,转e)。

d)根据索引表 table,依次查找每个训练矢量在码书中的 相应码字,并将相应的码字转换成大小为 n×n 的图像子块, 最后将所有图像子块还原成原始图像。

e)根据索引表 table,依次查找与每个训练矢量相对应的 码字 c_j ,如果 $c_j \in P^0$,则令 $\omega'_i = 0$;若 $c_j \in P^1$,则令 $\omega'_i = 1$ 。将 依次提取的水印矢量 $wm' = \{\omega'_0, \omega'_1, \dots, \omega'_{(w \times h) - 1}\}$ 转换成大 小为 $w \times h$ 的图像,并进行 Arnold 置乱,生成水印图像 WT'。



4 实验结果与分析

为验证本文算法的效果,选取四幅大小为 256 × 256 的图 像作为测试图像,32 × 32 二值图像作为水印图像,如图 3 所

示。采用峰值信噪比 PSNR 度量嵌入水印后的图像质量,采用 归一化相关值 NC^[13]评价提取的水印效果。



图3 测试图像和水印图像

$$NC = \sum_{i=0}^{M-1N-1} \left(w(i,j) \times w'(i,j) \right) / \\ \sqrt{\sum_{i=0}^{M-1N-1} w^{2}(i,j)} \times \sqrt{\sum_{i=0}^{M-1N-1} \sum_{j=0}^{W'(i,j)} w'^{2}(i,j)}$$
(3)

图4表示使用本文图像分类方法得到的区域分类结果。 光滑区、一般区和纹理区三个区域分别用不同的灰度值表示。 由图可以看出,本文方法较好地达到了对图像区域分类的目 的,为基于图像熵分类的码书设计算法提供了较好的分类 结果。



表1比较了在码书大小不同的条件下使用传统 LBG 算法 和本文算法所得到的嵌入水印图像的 PSNR 值。图5 和6 分 别表示码书为1 024 时嵌入水印的 Lena 图像和 Woman 图像。 对比表中的数据可以看到,图像质量与码书大小呈正相关。码 书越大,图像质量越高。同时,在码书大小相同的条件下,由本 文算法所得到的 PSNR 值要远远高于传统的 LBG 算法的 PSNR 值,并且码书越大,图像的 PSNR 值越高,图像的质量 越好。

表 1	采用不同码	书训练方法得	到的嵌入水	印后的图像	PSNR 值
-----	-------	--------	-------	-------	--------

图像	初书训练子社	码书大小		
名称	的书训练力法	256	512	1 024
	LBG 算法的 PSNR 值	32.44	33.39	34.23
Lena	本文方法的 PSNR 值	33.90	34.22	37.22
	LBG 算法的 PSNR 值	34.28	35.14	35.84
Zelda	本文方法的 PSNR 值	35.25	36.69	38.97
XX 7	LBG 算法的 PSNR 值	33.72	34.36	35.92
Woman	本文方法的 PSNR 值	35.77	37.38	39.09
	LBG 算法的 PSNR 值	33.14	34.00	34.85
Pepper	本文方法的 PSNR 值	33.33	35.03	36.53

表 2 将本文算法得到的结果与文献[14]中的实验结果进行比较。其中,文献[14]选用的是 512 × 512 的 Lena 图像和 64 × 64的水印图像。由表 2 可知, Lena 图像在码书大小相同的条件下,本文算法得到的 PSNR 值高于文献[14]中的结果。 表 2 本文算法与文献[14]算法关于嵌入水印后图像 PSNR 值的比较

码书大小	128	256	512	1 024
本文算法得到的 PSNR 值	34.05	35.19	35.70	36.46
文献 [14] 中的 PSNB 值	29.43	30.97	32.00	32.62

以 Lena 图像为例,表 3 列出了对图像进行多种图像处理 得到的实验结果。由表 3 中可知,本算法对 JPEG 压缩,具有 较强的抗压缩能力;对图像剪切,即使在剪切 1/2 的情况下,提 取的水印 NC 值仍能达到 70%;对于其他图像攻击,提取的水

表 3 对图像进行各种处理后提取水印的 NC 值					
图像处理	NC 值	图像处理	NC 值		
JPEG 压缩(质量品质 90)	0.998 8	均值滤波(2×2)	0.829 2		
JPEG 压缩(质量品质 60)	0.967 9	中值滤波(3×3)	0.868 8		
JPEG 压缩(质量品质 20)	0.824 3	旋转 0.1°	0.996 0		
剪切左上角 1/4	0.868 2	旋转 0.5°	0.841 0		
剪切周边 1/4	0.864 2	缩放(先缩小0.5 倍再放大2倍)	0.867 3		
剪切 1/2	0.711 6	锐化两次	0.889 9		
椒盐噪声(方差0.04)	0.858 4	对比度增加10	0.918 6		

为破坏嵌入到图像中的水印,除了对嵌入水印后的图像本 身进行攻击外,攻击者还可能在图像传输中对码书和索引值进 行窜改。如在索引表中将索引值删除或使用其他图像的码书 来代替等方式进行攻击。

表4表示在图像传输的过程中,窜改索引表中索引值后提 取得到的水印 NC 值。由表4 可见,当被窜改的索引值个数较 少时,本算法具有较强的抗干扰能力;且索引值个数改变越少, 则 NC 值越大,提取水印的效果越好。

表 4	修改索引表提取水印得到的 NC	佰
45 T		

	1
窜改索引值	NC 值
将前100个索引值置1	0.989 6
将前 256 个索引值置 1	0.970 2
将前 512 个索引值置 1	0.937 6
将前1024个索引值置1	0.864 2
将前1229个索引值置1	0.8337
(占全部索引值的30%)	

表 5 表示将图像的码书进行窜改,提取得到的水印 NC 值。分析表 5 可知,若使用一幅图像的码书窜改另一幅图像的 码书,如果两幅图像之间的差异度较小,即两者的码书较相似, 则提取出的水印效果较好;若两者差异度较大则提取出的水印 效果较差。

5	窜改图	1像码书	后提取水	、印得到的	NC 值

窜改方式	NC 值
用 Woman 图像 1/16 码书代替 Lena 图像 1/16 码书	0.953 7
用 Woman 图像 1/8 码书代替 Lena 图像 1/8 码书	0.919 5
用 Woman 图像 1/4 码书代替 Lena 图像 1/4 码书	0.879 5
用 Pepper 图像 1/16 码书代替 Lena 图像 1/16 码书	0.932 1
用 Pepper 图像 1/8 码书代替 Lena 图像 1/8 码书	0.901 1
用 Pepper 图像 1/4 码书代替 Lena 图像 1/4 码书	0.863 6

5 结束语

表

本文针对码书设计过程中不能自适应的根据不同图像特 征区域进行量化编码的缺点,提出了一种改进的矢量量化盲数 字水印算法。采用的基于图像分类方法的码书生成算法在保 证图像具有较高压缩比和较快编码速度的基础上,使重建图像 具有更高的质量。同时,通过在水印提取过程中对码书进行的 预处理,使水印更具有健壮性。实验证明,本文算法简单、高 效,对常见的各种图像攻击具有较强鲁棒性。

参考文献:

- [1] 马文龙,余宁梅. 图像块动态划分矢量量化[J]. 计算机辅助设 计与图形学学报,2005,17(2):279-284.
- [2] LU Z W, SUN S H. Digital image watermarking technique based on vector quantization[J]. Electronics Letters, 2000, 36(4): 303-305.

n呈线性关系,这里n是参与者的秘密向量的长度。协议具体的计算和通信复杂度如表1所示。

表1	协议的计算和通信复杂度分析
----	---------------

操作	第一阶段	第二阶段
	乘积协议:0(n)	同态加解密操作:O(n)
计算复杂度(Alice)	模乘运算:0(n)	模乘运算:0(1)
	幂模运算:0(n)	幂模运算:0(1)
通信复杂度(Alice)	O(n)	O(n)
	乘积协议:0(n)	同态加密操作:O(n)
计算复杂度(Bob)	模乘运算:0(n)	模乘运算:0(n)
	幂模运算:0(n)	幂模运算:0(1)
通信复杂度(Bob)	O(n)	O(n)

3 结束语

本文利用同态加密的特殊性质和基于健忘传输的保密两 方乘积协议构造了一个恶意模型下安全的保密两方共享点积 协议。同以前的有关协议相比,该协议的安全性更高,不仅在 半诚实模型下是安全的,而且在有恶意参与者存在的情况下也 是安全的。它为许多保密数据挖掘协议的设计提供了更高的 安全保证。在后面的工作中,将进一步探讨多方保密点积协议 的设计问题,并研究将保密点积协议应用于保密集合相交问题 及其他计算几何问题中。

参考文献:

- YAO A C. Protocols for secure computation [C] //Proc of the 23rd Annual Symposium on Foundations of Computer Science. Washington DC: IEEE Computer Society, 1982: 160-164.
- [2] GOLDREICH O, MICALI S, WIGDERSON A. How to play any mental game [C] //Proc of the 19th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1987: 218-229.
- [3] CHAUM D, CREPEAU C, DAMGARD I. Multiparty unconditionally secure protocols[C] //Proc of the 20th Annual ACM Symposium on Theory of Computing (STOC'88). New York: ACM Press, 1988: 11-19.
- [4] LUO Wen-jun, LI Xiang. A study of secure multi-party elementary function computation protocols[C] //Proc of the 3rd International Conference on Information Security. New York: ACM Press, 2004: 5-12.
- [5] LUO Wen-jun, LI Xiang. A study of secure multi-party statistical analysis [C] //Proc of International Conference on Computer Networks and Mobile Computing. Washington DC: IEEE Computer So-

- [3] LIN Y C, HUANG Z K, PONG T T. A robust watermarking scheme combined with the FSVQ for images [C]//Proc of International Conference on Information Technology and Applications. 2005;597-602.
- [4] WANG F H, JAIN L C, PAN J S. A novel SVD and VQ-based image hiding scheme [J]. Pattern Recognition Letters, 2001, 22 (9): 1051-1058.
- [5] LINDE Y, BUZO A, GRAY R M, et al. An algorithm for vector quantizer design [J]. IEEE Trans on Communications, 1980, 28 (1): 84-95.
- [6] SHEN F, HASGAWA O. An adaptive incremental LBG for vector quantization[J]. Neural Networks, 2006, 19(5):694-704.
- [7] MA C K, CHAN C K. A fast method of designing better codebooks for image vector quantization [J]. IEEE Trans on Communications, 1994, 40(4): 237-242.
- [8] KRISHNAMARTHY A K, AHALT S C, MELTON D E, et al. Neural networks for vector quantization of speech and images [J]. IEEE Journal on Selected Areas Communications, 1990, 8 (8):

ciety, 2003: 377-382.

- [6] GOLDWASSER S. Multi-party computations: past and present[C] //Proc of the 16th Annual ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 1997: 1-6.
- [7] VERYKIOS V S, BERTINO E, FOVINO I N, et al. State-of-the-art in privacy preserving data mining [C] //Proc of ACM SIGMOD Record. New York: ACM Press, 2004: 50-57.
- [8] LINDELL Y, PINKAS B. Privacy preserving data mining[C] //Proc of the 20th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer-Verlag, 2000: 36-54.
- [9] PINKAS B. Cryptographic techniques for privacy-preserving data mining[C] //Proc of ACM Special Interest Group on Knowledge Discovery and Data Mining (SIGKDD). New York: ACM Press, 2002: 12-19.
- [10] JAGANNATHAN G, WRIGHT R N. Privacy-preserving distributed K-means clustering over arbitrarily partitioned data[C] //Proc of the 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining. New York: ACM Press, 2005: 593-599.
- [11] VAIDYA J, CLIFTON C. Privacy preserving association rule mining in vertically partitioned data [C] //Proc of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM Press, 2002: 639-644.
- [12] ATALLAH M J, DU Wen-liang. Secure multi-party computational geometry[C] // Proc of the 7th International Workshop on Algorithms and Data Structures. London, UK: Springer-Verlag, 2001: 165-179.
- [13] DU Wen-liang, ATALLAH M J. Privacy-preserving cooperative statistical analysis[C] //Proc of the 17th Annual Computer Security Applications Conference. Washington DC: IEEE Computer Society, 2001: 102-110.
- [14] ELGAMAL T. A public-key cryptosystem and a signature scheme based on discrete logarithms [C] //Proc of CRYPTO'84 on Advances in Cryptology. New York: Springer-Verlag, 1985: 10-18.
- [15] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes [C] //Proc of Advances in Cryptology-EURO-CRYPT'99. Berlin, Heidelberg; Springer-Verlag, 1999; 223-238.
- [16] DU Wen-liang, ATALLAH M J. Privacy-preserving cooperative scientific computations [C] //Proc of the 14th IEEE Computer Security Foundations Workshop. Washington DC: IEEE Computer Society, 2001: 273-282.

1449-1457.

- [9] PAN J S, SUNG M T, HSIANG C H. Robust VQ-based digital watermarking for memoryless binary symmetric channel [C]//Proc of International Symposium on Circuits and Systems. 2004: 580-583.
- $[\,10\,]$ EQUITZ W H. A new vector quantization clustering algorithm $[\,J\,]$. IEEE Trans on Acoustics Speech and Signal Processing , 1989 , 37(10):1568-1575.
- [11] 高珍,张伟,张志浩. 一种新的基于图块分类的水印算法[J]. 计算机工程, 2005, 31(24):177-180.
- [12] LUO Bin, GU Wei, GUO Hui. A VQ digital watermark algorithm based on T-mixture models segmentation [C]//Proc of IEEE Conference on Neural Networks and Signal Processing. 2008: 353-358.
- [13] 唐建. 矢量量化码书设计与矢量量化应用研究[D]. 合肥:中国 科学技术大学, 2006.
- [14] WU H C, CHANG C C. A novel digital image watermarking scheme based on the vector quantization technique [J]. Computers and Security, 2005, 24(6): 460-471.

⁽上接第2740页)