一种带纠错编码的小波域自适应盲水印算法

刘会英,张政保,文家福,李占德
(军械工程学院 计算机工程系,河北 石家庄 050003)

摘 要:文中提出了一种小波域自适应盲水印算法。该算法具有如下特点:(1)以图像局部相关特性为基础,采用块均值量化策略;(2)以人眼视觉掩蔽特性为基础,将小波系数块进行分类,不同类的块选取不同的量化步长,并且水印嵌入过程中块内系数的改变量自适应于系数本身大小;(3)利用纠错编码和混沌置乱对水印信息进行调制,以提高水印的鲁棒性。该算法在检测时不需要原始图像,实现了盲检测。实验结果表明,该方案能很好地抵抗JPEG压缩,叠加噪声,裁剪等攻击,具有良好的鲁棒性和透明性。

关键词:块均值量化;小波变换;纠错编码;混沌置乱
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2010)03-0140-03

A Wavelet Domain Adaptive Blind Watermarking Algorithm with Error Correcting Encoding

LIU Hui-ying, ZHANG Zheng-bao, WEN Jia-fu, LI Zhan-de
(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: A novel adaptive digital image watermarking algorithm in wavelet domain is proposed. The features of this algorithm are as follows: (1)Block quantization strategy based on local image characteristic is adopted. (2)Block in low-frequency band is classified into several classes based on human visual system. Different kind of block select different quantization step. During the embedding process, the change of coefficient in each block is adaptive to the absolute value of the coefficient itself. (3)In order to improve robustness of the watermark, error correction coding and chaos scrambling are adopted to modulate the watermark. The watermark can be detected without resorting to the original host image. Experiment results show that this scheme is proved of high invisibility and robustness.

Key words: block quantization; wavelet transform; error correction encode; chaos scrambling

0 引 言

随着计算机网络和通信技术的飞速发展,数字媒体已得到广泛的应用,随之而来的数字媒体的信息安全、知识保护和认证等问题也变得日益突出。数字水印作为传统加密方法的有效补充,是一种可以在开放网络环境下保护版权和认证来源及完整性的新技术。鲁棒性和不可感知性是对水印系统的基本要求,而影响不可感知性和鲁棒性的因素主要是水印的嵌入和检测策略。其中,采用量化策略的数字水印技术以其盲检测、计算简单、容易实现等特点,得到了普遍关注。

目前所采纳量化策略的水印算法大多存在以下不足[1]:

(1)对于采用的单系数量化的方式,忽略了图像自身局部相关特性,影响了水印的隐藏效果;

(2)现有的量化方案大多采用均匀量化[2],未能充分利用图像自身特点以及人眼视觉特性,因而透明性和鲁棒性有待进一步提高。

针对以上不足,笔者首先根据视觉掩蔽特性对小波低频系数块进行相应分类,然后针对不同的块类别选取不同的量化步长并以块均值量化的方式嵌入水印,同时结合纠错编码进一步提高水印的鲁棒性。实验表明该算法具有良好的不可感知性和鲁棒性。

1 纠错编码

纠错编码本质是通过向原始信息中增加冗余信息,以使得信息在传输过程中尽可能减少误码。文中采用(7,4)汉明码对水印进行处理,它是可以纠正所有单个随机错误的高效率线性分组码。(7,4)汉明码特点:码长:$n=7$;信息码位:$k=4$;监督码位:$r=3$;最

收稿日期:2009-06-27;**修回日期**:2009-09-28
基金项目:河北省科技厅基金资助项目(05213579)
作者简介:刘会英(1984-),男,硕士研究生,研究方向为信息安全、图像加密;张政保,教授,硕士生导师,研究方向为信息安全、多媒体信息处理。

小码距:$d = 3$;纠错能力:$t = 1$。

发送码组 A 在传送过程中可能发生误码,收到的码组为 B,收发码组 $B - A = E$:

$$E = [e_{n-1}, e_{n-2}, \cdots, e_0] \quad e_i = \begin{cases} 0 & b_i = a_i \text{ 无错} \\ 1 & b_i \neq a_i \text{ 有错} \end{cases} \tag{1}$$

接收端计算校正子 S 为:

$$S = BH^{\mathrm{T}} = (A + E)H^{\mathrm{T}} = AH^{\mathrm{T}} + EH^{\mathrm{T}} = EH^{\mathrm{T}}$$

H 为监督矩阵,错误图样与校正子有确定的关系。

2　混沌映射

混沌现象是非线性系统中出现的确定性的类似随机的过程。

Logistic 映射是典型的,广为应用的一维混沌模型[3],其函数如式(2)所示。式(2)中 μ 属于[0 4],$x_k \in (0\ 1)$。当 $3.569945 < \mu < 4$ 时,Logistic 映射工作处于混沌状态,也就是说给定不同的初值 x_0 时,由式(2)生成的序列非周期,不收敛,不相关。

$$x_{k+1} = \mu x_k(1 - x_{k+1}) \tag{2}$$

利用式(2)可以很方便地生成混沌序列。混沌序列作为一种伪随机序列,具有生成形式简单,对初始条件极其敏感,具备白噪声的统计特性,且不具有逆推性,因而可以在数字水印技术中得到广泛应用。运用混沌序列对水印信息进行置乱,是其中的一种应用。这里的水印信息一般为二值或灰度图像,置乱的目的是去除水印的相关性以及增强水印算法的鲁棒性。

3　水印的嵌入和提取算法

3.1　嵌入位置的选择

对于小波域水印算法而言,水印的嵌入位置对算法的透明性和鲁棒性具有重要的影响。Cox 等认为图像水印应放在视觉上最重要的位置上[4]。视觉上重要的分量是图像信号的主要成分,图像信号的大部分能量都集中在这些分量上,在图像有一定失真的情况下,仍能保留主要成分,即视觉上重要的分量的抗干扰能力较强。因此,将水印嵌入小波低频系数能获得较好的鲁棒性。虽然人眼对于低频系数变化比较敏感,但如果能充分利用人眼的视觉掩蔽特性,合理地选取水印的量化步长,就能较好地实现水印鲁棒性和透明性之间的平衡。综上所述,文中选择小波低频子带进行水印嵌入。

3.2　HVS 理论下量化步长的确定

在信息隐藏中应用人眼视觉特性,主要是利用人眼的一些视觉掩蔽特性,如人眼对于微小的亮度变化不能察觉,对图像平滑区和边缘区域噪声比较敏感,而在纹理区对噪声不敏感等[5,6]。因此,文中根据块亮度大小(用能量大小描述)及纹理复杂程度(用方差描述)[7,8]将小波低频系数子块划分为三类不同的噪声敏感区,然后对于每一类选取相应的量化步长。设载体图像 $I = \{g(i,j), 1 \leq i < M, 1 \leq j < M\}$,二值水印 $W = \{w(i,j), 1 \leq i < P, 1 \leq j < Q\}$。具体过程:首先将载体图像 L 级小波分解后的逼近子带划分为大小为 $N \times N$ 的小波系数子块,然后利用式(3)、(4)计算各块的能量大小 E 及方差 D,再利用式(5)来确定全局阈值,最后通过式(6)对各子块进行分类并确定相应量化步长 q。e_i 为小波系数块内系数值大小。

能量公式:$E = \sum_{i=1}^{N^2} e_i^2$ (3)

方差公式:$D = \sum_{i=1}^{N^2} (e_i - \sum_{i=1}^{N^2} e_i / N^2)^2 / N^2$ (4)

阈值设定:

$$\begin{aligned} T1 &= (E_{\max} - E_{\min}) \times 0.9 + E_{\min} \\ T2 &= (E_{\max} - E_{\min}) \times 0.1 + E_{\min} \\ T3 &= (D_{\max} - D_{\min}) \times 0.9 + D_{\min} \\ T4 &= (D_{\max} - D_{\min}) \times 0.1 + D_{\min} \end{aligned} \tag{5}$$

量化步长确定:

$$q(m,n) = \begin{cases} q_1, E(m,n) > T1 \text{ 且 } D(m,n) > T3 \\ q_2, E(m,n) < T2 \text{ 且 } D(m,n) < T4 \\ q_3 \qquad\qquad \text{其余子块} \end{cases} \tag{6}$$

3.3　水印的嵌入

(1) 纠错编码。将二值水印图像 W 进行水平扫描得到长度为 $P \times Q$ 的一维向量,然后以每 4 位为一组进行纠错编码后得到 $W1$。对 $W1$ 进行填充至长度为 $M^2/(4^l \times N^2)$。

(2) 混沌置乱。利用式(1)产生与 $W1$ 长度相同的混沌序列 X,使 X 与 $W1$ 一一对应。通过冒泡法将 X 按从大到小的顺序排列,同时与 X 一一对应的 $W1$ 序列也被置乱。

(3) 量化步长的确定。将载体图像 I 进行 L 级 Haar 小波变换,然后将小波逼近子带划分为大小 $N \times N$ 的小波系数块,最后依据上述的系数块分类方法进行分类,并确定相应量化步长。量化步长具体取值依据图像的不同通过实验仿真选取。

(4) 量化嵌入。以块均值量化的方式对每个系数块嵌入一比特水印信息。设待嵌入水印的小波系数块 $B = \{b(i,j), 1 \leq i < N, 1 \leq j < N\}$,$r$ 为块绝对值均值,r' 为修改后的块绝对值均值,q 为相应的量化步长,$W1(i)$ 为待嵌入水印信息。具体实现如下:

$$\text{if } W1(i)=1:\begin{cases} r'=r-\text{mod}(r,q)-q/4 \\ \text{mod}(r,q)\le q/4 \\ r'=r-\text{mod}(r,q)+3*q/4 \\ \text{mod}(r,q)>q/4 \end{cases} \tag{7}$$

$$\text{if } W1(i)=0:\begin{cases} r'=r-\text{mod}(r,q)+5*q/4 \\ \text{mod}(r,q)\ge 3*q/4 \\ r'=r-\text{mod}(r,q)+q/4 \\ \text{mod}(r,q)<3*q/4 \end{cases} \tag{8}$$

假定 $\Delta = r' - r$,则经修改后的块内各系数值:

$$\begin{cases} \text{if } b(i,j)>0\ b(i,j)'=b(i,j)+\dfrac{\Delta * b(i,j)}{r} \\ \text{if } b(i,j)\le 0\ b(i,j)'=b(i,j)+\dfrac{\Delta * b(i,j)}{r} \end{cases} \tag{9}$$

(5) 重复(4) 直到所有系数块均已嵌入水印,对修改后的系数作小波逆变换,得到嵌入水印的图像 I'。

3.4 水印的提取

水印的提取过程是嵌入的逆过程。先对含水印图像 I 进行 L 级 Harr 小波分解,将 L 级小波逼近子带分块($N\times N$),并依据上述分类方法确定各块的量化步长 q,然后按式(10) 从各系数块中提取水印信息 $W(i)$。当所有块中水印都被提取后,将 W 进行纠错解码、反置乱及行列变换,即可得到提取的水印图像。

$$W(i)=\begin{cases} 0 & \text{mod}(r,q)\le q/2 \\ 1 & \text{mod}(r,q)>q/2 \end{cases} \tag{10}$$

4 实验结果与分析

文中用大小为 512×512 的 256 灰度 Lena 图像进行水印嵌入和提取的仿真实验,采用大小为 16×32 的二值图像作为数字水印,如图 1(b)。图 2(a)为含水印图像,图 2(b)为提取的水印图像。其中 L 取 2,N 取 4;q_1,q_2,q_3 分别取 10,22,34(通过实验选取);μ 取 3.9,混沌初值 x_0 取 0.32568。

(a) 原始图像 (b)原始水印

图 1 原始图像及水印

实验中对水印图像进行了中值滤波(3×3),剪切 1/4,中心裁剪,叠加高斯噪声,叠加椒盐噪声,缩放,20%的 JPEG 压缩等攻击。用归一化相关系数 NC 衡量提取水印与原始水印的相关度。从图 3 和表 1 可以看出,本算法具有良好的透明性并且对各种常见攻击具有很好的鲁棒性。和文献[2]中的算法相比,在滤波,叠加噪声,JPEG 压缩攻击及缩放攻击等方面鲁棒性明显增强。

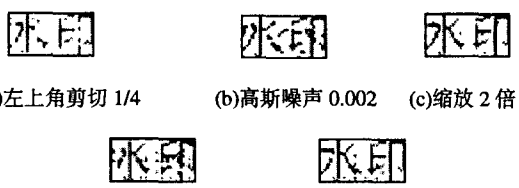
(a)含水印图像 (b)提取水印

psnr = 44.1474 NC=1

图 2 含水印图像及提取水印

表 1 两种算法抗攻击能力比较

操作	文献[2]算法		文中算法	
	PSNR/dB	NC	PSNR/dB	NC
无攻击	40.3598	1	44.1474	1
0.001 高斯噪声	29.6269	0.7484	29.8150	0.9776
0.002 高斯噪声	26.8186	0.5809	26.8970	0.8361
0.01 椒盐噪声	25.0670	0.7626	25.3921	0.8535
3×3 中值滤波	30.7717	0.7806	34.9032	0.9455
20%JPEG 压缩	29.5589	0.5296	32.6199	0.8123
缩放 2 倍	27.7405	0.7025	31.8907	0.9626
左上角剪切 1/4	10.1285	0.8956	11.7972	0.8997
中心裁剪	12.6469	0.8892	14.6927	0.8905



(a)左上角剪切 1/4 (b)高斯噪声 0.002 (c)缩放 2 倍

(d)20%JPEG 压缩 (f)3×3 中值滤波

图 3 各种常见攻击下提取的水印

5 结束语

文中将纠错编码应用于图像水印编码中,并结合人眼视觉掩蔽特性提出了一个基于块分类的小波域盲水印算法,所实现的水印具有以下优点:

(1)采用汉明码对水印进行纠错编码,并利用混沌序列对纠错编码后水印信息进行混沌置乱,提高了水印的鲁棒性和安全性。

(下转第 146 页)

减规则为先设定 max_des_support 为上层最小支持度,其次为每隔两层取上层最小计数为次层的最小支持度。已知特征长度取 4。实验结果如图 2 所示。

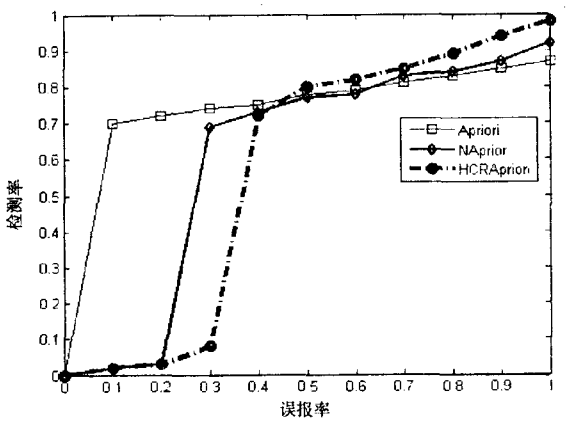


图 2 误报率检测率性能对照图

实验分析:结果显示,使用具有递减支持的 HCRApriori 算法比 Apriori 算法 和 NApriori 算法具有较高精确的检测性能。同样的检测率下,HCRApriori 算法比其他两个算法具有更低的误报率。在试验中,也发现使用较短特征曲线的检测率比较长特征曲线的检测率要高。原因是正常流量中的较短特征出现的概率偏高,但会导致较高的误报率。

5 结束语

文中提出了一种基于规则约束制导的数据挖掘算法,利用已知特征来检测现有入侵模式的变异事件,在此基础上加入递减支持度,以免忽略低支持度事件有可能也是兴趣事件。本算法在消耗时间上大幅度降低和在误报率检测率上都有很好的改进。递减支持度规则的优越性,直接影响到检测率的高低。如何选取更优越的递减支持度规则是笔者下一阶段的研究方向。

参考文献:

[1] 阮耀平,易江波. 计算机系统入侵检侧模型与方法[J]. 计算机工程,2005,28(11):232-236.

[2] 高海华,王行愚,杨辉华. 基于群智能和 SVM 的网络入侵特征选择和检测[C]//2005 年中国智能自动化会议论文集[C]. 北京:国防工业出版社,2005:111-114.

[3] 彭竹苗,张正道,白瑞林,等. 基于 HMM 模型的网络入侵误用检测方法[C]//2007 中国控制与决策学术年会论文集. 沈阳:东北大学出版社,2007:67-70.

[4] 王玉震,李 雷. 基于 SVR 的图像增强方法[J]. 计算机技术与发展,2009,19(1):60-62.

[5] Hu Zhengbing, Li Zhitang, Wu Junqi. A novel network intrusion detection (NIDS) based on signatures search of data mining[C]//2008 Workshop on Knowledge Discovery and Data Mining. Moscow, Russia:[s.n.],2008:10-16.

[6] Agrawal R, Imieilnski T, Swami A. Mining association rules between sets of items in large databases[C]//Proc of the ACM SICMOD Int Conf on Management of Data. Washington DC:[s.n.],1993:207-216.

[7] Han J W, Pei J, Yin Y. Mining frequent paterns without candidate generation[C] //Proc of the 2000 ACM SIGMOD Int Conf on Management of Data. Dallas:[s.n.],2000:1-12.

[8] Agrawal R, Srikant R. Fast algorithms for mining association rules[C]//Proc of the 20th Into Conf Very Large Data Bases. Santiago, Chile:[s.n.],1994:487-499.

[9] 韩家炜,坎 伯. 数据挖掘:概念与技术[M]. 范 明,孟小峰译. 北京:机械工业出版社,2001:152-157.

[10] KDD (1999), the third international knowledge discovery and data mining tools competition data set (KDD99 Cup)[EB/OL]. 1999. http://kdd. ics. uci. edu/databases/kddcup99. html.

(上接第 142 页)

(2)利用人眼掩蔽特性根据小波低频系数块所属类别选取相应的量化步长,并且水印嵌入过程中块内系数的改变量自适应于系数本身大小,具有较好的自适应性。

(3)对各种常见攻击具有良好的鲁棒性,并且水印的提取不需要原始图像,具有较好的实用性。

参考文献:

[1] 董 敏,王向阳. 基于分块量化的小波域数字水印嵌入算法[J]. 微电子学与计算机,2007,24(7):31-34.

[2] Masry M, Ramos M, Hemami S. Robust data hiding using psychovisual thresholding[C]//ICIP2000 Proc 2000 Int Conf Image Processing. Vancouver, Canada: IEEE Signal Processing Society,2000:593-596.

[3] Cox I J, Killian J. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997,6(12):1673-1690.

[4] 李赵红,侯建军. 基于 Logistic 混沌映射的 DCT 域脆弱数字水印算法[J]. 电子学报,2006,34(12):2134-2137.

[5] Sepsirisuk K. An adaptive digital watermarking based on a tree structure using the human visual system[J]. IEEE IN T,2005 (2):1062-1065.

[6] Nillnb A. Visual model weighted cosine transform for image compression and quality assessment[J]. IEEE Transaction on Communications,1995,33(6):551-557.

[7] 朱兴力,张家树. 基于小波系数块能量分析的自适应数字水印算法[J]. 计算机应用,2006,26(4):830-832.

[8] Liu Hongmei, Huang Jiwu. An adaptive video watermarking algorithm in wavelet domain[J]. Acta Electronica Sinica, 2001,29(12):1656-1660.