

基于整数小波矩阵范数量化的多重数字水印算法

刘新^{1,2},王英²,杨国为²

LIU Xin¹,WANG Ying²,YANG Guo-wei²

1.黑龙江科技学院 电气与信息工程学院,哈尔滨 150027

2.青岛大学 自动化工程学院,山东 青岛 266000

1.School of Electronic Information Engineering,HIST,Harbin 150027,China

2.School of Automation,Qingdao University,Qingdao,Shandong 266000,China

E-mail:LX2001.LX@163.com

LIU Xin,WANG Ying,YANG Guo-wei.Multiple digital watermarking algorithm based on integer wavelet matrix norm quantization.Computer Engineering and Applications,2007,43(34):108-110.

Abstract: A multiple digital watermarking algorithm is proposed to complete multi-sexual and multi-type of protecting multimedia information.In integer wavelet domain,robust watermarks are embedded into low frequency zone and fragile watermarks into different layers progeny details by the quantization method of matrix norm.Watermarks can be detected in different layers, which is a blind detecting algorithm.Experiments show that the algorithm not only has both robustness and fragile sensitivity,but also exactly locates distorted part.It is an effective watermarking algorithm.

Key words: multiple digital watermarks;integer wavelet;matrix norm quantization;SVD;chaotic scrambling

摘要:针对多媒体版权信息保护的多方性和多类性,提出一种多重数字水印算法。在整数小波域,利用矩阵范数量化方法,将鲁棒水印嵌入到逼近子带,将脆弱水印嵌入到细节子带,水印提取检测可分层进行,且为盲检测。仿真表明,该算法兼具鲁棒性和敏感性,且能够较精确反映篡改区域,是一种有效的多重数字水印方案。

关键词:多重水印;整数小波;矩阵范数量化;奇异值分解;混沌置乱

文章编号:1002-8331(2007)34-0108-03 **文献标识码:**A **中图分类号:**TP391

1 引言

数字水印技术在多媒体数据保护方面的应用,得到了高度重视,其发展在不断深化。在实际应用中,多媒体数据版权信息的多方性(如原创者、发行商、授权使用者等)和版权保护的多类性(如版权认证、盗版跟踪、数据真伪等),希望嵌入多重水印。但目前对于多重数字水印算法的研究并不多见,Thai Duy Hien 等人^[1]提出一种在小波域嵌入多重脆弱水印的认证水印算法;华先胜等人^[2]对比多类水印嵌入顺序,提出将多类水印同时嵌入;王英等人^[3]提出一种多重水印的零嵌入方法。

多重水印同时嵌入,这无疑进一步加剧了水印不可见性、鲁棒性、可证明性之间的矛盾,其技术特点在于:

(1)各水印信号既要尽可能简单,又要极具代表意义,以保证不发生法律歧义,发挥各阶段的法律作用;

(2)所要隐藏的信息量大,势必增大视觉隐蔽难度,水印的不可见性和鲁棒性的均衡问题更加尖锐;

(3)若各水印嵌入不独立还将导致检测的互相干扰,难于保证按需提取。

针对上述问题,本文以静止图像为研究对象,提出在整数

小波域,利用矩阵范数量化法实现鲁棒水印和脆弱水印综合嵌入,实现数字水印对多媒体数据的版权保护、完整性认证等多法律效用。

2 相关理论

2.1 整数小波变换

在实际应用中,传统的小波变换存在一些问题:传统小波变换是浮点数运算,计算机有限字长将引入舍入误差,往往不能精确的重构信号;计算量大,计算复杂度高,对存储空间的要求高,不利于硬件实现。为克服上述问题,引入了整数小波变换(LWT)。它不依赖于傅立叶变换,仍继承传统小波多分辨特性,且变换后系数是整数,计算速度较快,无需额外的存储开销,被誉为第二代小波。整数小波变换是将现有的小波滤波器分解成基本的构造模块,经过分裂、预测和更新三步来完成小波变换,如图1所示。

整数小波变换在数字水印技术中的应用,除了具备传统小波变换的优点外,还具有以下优点:

(1)避免了数学变换中由浮点数引起的舍入误差;

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60673101)。

作者简介:刘新(1983-),男,硕士研究生,主要研究领域:信息安全、数字水印等;王英(1959-),女,博士,教授,研究生导师,主要研究领域:混沌及网络安全信息、算法设计等;杨国为(1964-),男,博士,教授,研究生导师,主要研究领域:人工智能、人工生命、人工神经网络、模式识别、创新设计等。

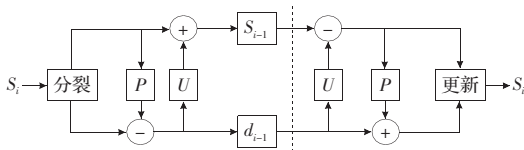


图1 整数小波变换分解和重构示意图

(2)计算速度快,不需要额外的存储开销。

2.2 矩阵奇异值与矩阵范数

矩阵的奇异值分解(SVD)是一种正交变换,它可以将矩阵对角化,即

若矩阵 $A \in R^{m \times n}$ 非负,则使得

$$A=USV^T \quad (1)$$

$$U^TAV=S=diag(\sigma_1, \sigma_2, \sigma_3, \dots, \sigma_p) \quad (2)$$

其中 $p=\min(m, n)$, σ_i 称为 A 的奇异值且 $\sigma_1 \geq \sigma_2 \geq \sigma_3 \geq \dots \geq \sigma_p$, U, V 分别是 S 的左右奇异值向量。

非负矩阵 A 的谱范数(2-范数)和 F-范数表示如下:

$$\|A\|_2 = \sqrt{\lambda_{\max}(A^T A)} = \sigma_1 \quad (3)$$

$$\|A\|_F = \sqrt{\sum_{i=1}^m \sum_{j=1}^n a_{ij}^2} = \sqrt{\sum_{i=1}^p \lambda_i} = \sqrt{\sigma_1^2 + \sigma_2^2 + \dots + \sigma_p^2} \quad (4)$$

可以看出,矩阵的谱范数是奇异值的最大值,矩阵的 F-范数是所有奇异值的平方和,矩阵范数与奇异值存在一定的对应关系。

将 SVD 引入到数字水印算法中来^[4-6],其理论依据在于:

- (1)奇异值分解对图像尺寸无限制;
- (2)图像奇异值的稳定性非常好,即当图像被施加小的扰动时,其奇异值不会发生剧烈的改变。

通过改变奇异值来实现水印的嵌入,可以提高水印算法的鲁棒性,但是计算 SVD 增加了算法的复杂度和计算量。由式(3)、式(4),修改矩阵奇异值,矩阵的谱范数和 F-范数也随之改变,不妨直接改变矩阵的范数来实现水印的嵌入。

3 一种利用矩阵范数量化实现的多类多重水印算法的设计

为了避免浮点数舍入误差,对宿主图像进行整数小波变换;鉴于图像逼近子带具有较强的鲁棒性、细节子带具有较好的敏感性,将鲁棒水印嵌入到逼近子带中,将脆弱水印嵌入到细节子带中;为了篡改定位,对各子带进行分块,求各块矩阵的谱范数,通过范数量化来嵌入水印;另外,为了提高算法的安全性,采用 Logistic 混沌序列对水印进行置乱加密。

嵌入过程如图 2 所示。

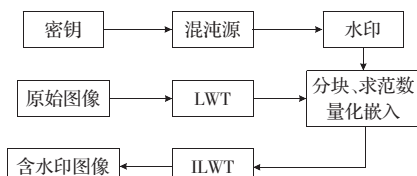


图2 水印的嵌入过程

步骤 1 水印混沌置乱加密。

Logistic 混沌系统:

$$x_{k+1} = \mu x_k (1 - x_k) \quad (5)$$

式中分支参数 $\mu \in (3.569\ 945, 4]$, $x_k \in (0, 1)$ 。

初值 x_0 和分支参数 μ 作为密钥 $K(x_0, \mu)$,生成混沌序列 X

来置乱水印 W ,具体过程如下:

(1)将 X 按下式升序重排,得到升序混沌序列 X' 和索引序列 l ;

$$[X', l] = \text{sort}(X) \quad (6)$$

(2)将索引序列 l 按列转换成二维矩阵 L ;

(3)按置乱索引矩阵 L 重排原始水印 W ,得到置乱的水印 W' ;

步骤 2 整数小波变换。

选用 9-7 正交小波基将原始图像 I 进行 2 级整数小波变换,得到 7 个子带。将鲁棒水印嵌入到宿主图像小波域的逼近子带(LL_2)中,将中频脆弱水印嵌入到 HL_2, LH_2, HH_2 细节子带,将高频脆弱水印嵌入到 HL_1, LH_1, HH_1 细节子带;

步骤 3 水印嵌入。

(1)将所有子带进行 $q \times q$ 的分块,记为 $I_g \in R^{q \times q}$,求谱范数 $\|I_g\|_2$,并计算量化系数 $\lambda = \lfloor \frac{\|I_g\|_2}{\delta} \rfloor$ 和控制系数 $\gamma = \|I_g\|_2 - \lambda \delta$,其中 δ 为基于人类视觉掩蔽特性设定的量化步长;

(2)修改矩阵谱范数:

$$\text{若 } (\lambda + w_i') \bmod 2 = 1 \text{ 且 } \gamma < \frac{\delta}{2}, \text{ 记 } \|\tilde{I}_g\|_2 = (\lambda - \frac{1}{2})\delta;$$

$$\text{若 } (\lambda + w_i') \bmod 2 = 1 \text{ 且 } \gamma \geq \frac{\delta}{2}, \text{ 记 } \|\tilde{I}_g\|_2 = (\lambda + \frac{3}{2})\delta;$$

$$\text{否则,记 } \|\tilde{I}_g\|_2 = (\lambda + \frac{1}{2})\delta;$$

(3)采用等比同秩修正法^[7]:

$$\tilde{I}_g = I_g + t I_g \quad (7)$$

其中, t 为修正量,其值取为

$$t = \frac{\|\tilde{I}_g\|_2}{\|I_g\|_2} - 1$$

$$\text{则 } \tilde{I}_g = \frac{\|\tilde{I}_g\|_2}{\|I_g\|_2} I_g$$

步骤 4 进行 2 级整数小波逆变换得到含水印图像 I' 。

水印的提取是盲检测方案,具体过程如下:

步骤 1 将待检测图像 I'' 进行 2 级 9-7 正交小波基 LWT;

步骤 2 水印提取:

将每个子带进行 $q \times q$ 分块,每一块记为 I_g'' ,并计算其谱范数 $\|I_g''\|_2$ 和量化系数 $\lambda'' = \lfloor \frac{\|I_g''\|_2}{\delta} \rfloor$:

$$\text{若 } \lambda'' \bmod 2 = 1, \text{ 则 } w_i'' = 1;$$

$$\text{若 } \lambda'' \bmod 2 = 0, \text{ 则 } w_i'' = 0;$$

得到置乱的水印 W'' ;

步骤 3 水印检测:

将提取出的置乱水印进行解密,得到水印 W^* ,可以主观判断,也可通过相关检测函数(SIM)、峰值信噪比(PSNR)来判断提取出的鲁棒水印的真伪,通过篡改评估函数(T_{AF})来判断脆弱水印的篡改程度。

$$SIM(W, W^*) = \frac{\sum_{i=1}^m \sum_{j=1}^n (W(i, j) \times W^*(i, j))}{\sqrt{\sum_{i=1}^m \sum_{j=1}^n (W^*(i, j))^2}} \quad (8)$$

$$PSNR(W, W^*) = 10 \lg \left(\frac{255^2}{\sum_{i=1}^m \sum_{j=1}^n (W(i, j) \times W^*(i, j))^2} \right) \text{dB} \quad (9)$$



图4 破坏性涂改攻击



图5 平滑涂改攻击



图6 剪切攻击



图7 维纳滤波攻击



图8 JPEG压缩攻击



图9 加入高斯噪声攻击

表1 提取出的鲁棒水印SIM值和脆弱水印 T_{AF} 值

攻击类别	鲁棒水印相关值	中频脆弱水印可信度	高频脆弱水印可信度
破坏性涂改攻击	0.969 620 253 164 56	19.559 422 943 172 19	17.884 512 070 234 56
平滑涂改攻击	0.977 215 189 873 42	19.076 376 147 426 64	18.539 527 557 798 88
剪切攻击	0.941 772 151 898 73	18.246 633 796 779 01	17.239 932 177 965 37
维纳滤波攻击	0.994 936 708 860 76	5.975 594 901 012 86	2.252 075 058 830 57
80%JPEG压缩攻击	1.000 000 000 000 00	12.725 773 633 117 76	4.339 586 064 340 19
加入高斯噪声(方差为0.000 1)	1.000 000 000 000 00	17.092 699 609 758 30	14.961 951 356 669 80
加入椒盐噪声(方差为0.000 5)	0.994 936 708 860 76	11.907 560 210 979 40	11.714 508 659 025 50
加入乘性噪声(方差为0.001)	0.997 468 354 430 38	9.585 045 110 818 20	5.827 056 660 807 90

$$T_{AF}(W, W^*) = \frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n W(i, j) \oplus W^*(i, j) \quad (10)$$

4 实验仿真

在 Matlab7.0 平台上, 针对 Lena、Cameraman、Bamboo 等多幅灰度图像进行仿真, 以下给出 Lena(512×512)256 级灰度图像的一些仿真数据。图 3(a)为原始宿主图像, 图 3(b)二值水印, 依次为鲁棒水印、中频脆弱水印、高频脆弱水印, 图 3(c)为置乱水印图像, 图 3(d)为含水印图像。



图3 原始图像、水印图像、置乱水印和含水印图像

对含水印图像进行涂改攻击、剪切攻击、滤波处理、JPEG 压缩处理、加噪攻击等, 来检验算法的有效性。图 4 为破坏性涂改攻击, 图 5 为平滑涂改攻击(在 Lena 帽顶涂改), 图 6 为剪切攻击, 图 7 为维纳滤波攻击, 图 8 为 80%JPEG 压缩攻击, 图 9 为高斯噪声攻击。表 1 反映提取出的鲁棒水印相关检测值(SIM)和脆弱水印篡改可信度(T_{AF})。

无论是主观观察还是数值分析, 均可说明该算法嵌入的鲁棒水印具有很好的抗攻击能力, 而脆弱水印对攻击较敏感, 能够较准确地反映篡改的区域和篡改的频域特性。随着攻击程度的加大, 脆弱水印的失真也越来越大, 且对于同一攻击, 图像小波域的中频子带比高频子带鲁棒性好。

5 结束语

本文提出兼具版权保护和完整性认证的多重数字图像水

印算法, 其特点为:

- (1) 整数小波变换的利用, 减小了逆变换引入的舍入误差;
- (2) 各水印嵌入互不干扰;
- (3) 与奇异值计算相比, 矩阵范数量化方法可减少计算量;
- (4) 对子带进行分块, 更利于反映篡改区域;
- (5) 对水印进行混沌置乱加密, 在不增加水印信息量的前提下提高了算法的安全性。

仿真实验表明, 该算法对于常见攻击, 鲁棒水印具有良好的鲁棒性, 脆弱水印具有较理想的敏感性, 能克服同类水印技术中存在的鲁棒性和安全性缺陷, 可谓一种较为有效的水印算法。(收稿日期: 2007 年 7 月)

参考文献:

- [1] Hien T D, Nakao Z, Chen Yen-Wei. Robust multi-logo watermarking by RDWT and ICA[J]. Signal Processing, 2006, 86: 2981-2993.
- [2] 华先胜, 石青云. 多类水印的同时嵌入[J]. 北京大学学报: 自然科学版, 2001, 37(3): 305-314.
- [3] 王英, 郑德玲, 吴延华. 一种多重水印零嵌入算法[J]. 北京科技大学学报, 2006, 8: 799-802.
- [4] Zhou B, Chen J. A geometric distortion resilient image watermarking algorithm based on SVD[J]. Image and Graphics, 2004, 9(41): 506-512.
- [5] Bergman C, Davidson J. Unitary embedding for data hiding with the SVD[C]. Proc of SPIE on Security Steganography and Watermarking of Multimedia, San Jose, CA, 2005, 1: 568.
- [6] 张宪海, 杨永田. 基于 DFT-SVD 域抗几何攻击图像水印算法[J]. 计算机工程, 2006, 32(18): 120-122.
- [7] 李旭东, 张振跃. 利用矩阵范数实现的公开水印技术[J]. 计算机辅助设计与图形学学报, 2005, 17(8): 1757-1861.