

用于图像认证的安全可逆水印算法

吴晓云, 胡建军

(广东商学院 信息学院, 广东 广州 510320)

摘 要: 在图像中嵌入可逆水印时, 为了提高水印算法的安全性, 采用参数化整数小波并利用位于细节子带整数小波系数的特点, 提出了一种安全性高的可逆水印算法. 实验结果表明, 算法具有水印不可见性好、安全性高及篡改定位准确的特点.

关键词: 可逆水印; 图像认证; 安全性

中图分类号: TP319

文献标识码: A

文章编号: 1000-7180(2010)09-0037-03

A Secure Reversible Watermarking Algorithm for Image Authentication

WU Xiao-yun, HU Jian-jun

(School of Information Science, Guangdong University of Business Studies, Guangzhou 510320, China)

Abstract: By embedding reversible watermark, the original image can be recovered from the watermarked image when it is deemed to be authentic. To improve watermark security, a high secure reversible watermarking algorithm is proposed which adopts parameterized integer wavelet transform and the features of integer wavelet coefficients in the detail bands. Experimental results demonstrate the proposed scheme has good invisibility, high security and accurate localization for tampered area.

Key words: reversible watermarking; image authentication; security

1 引言

传统的用于认证的数字水印技术^[1-2]在图像通过真实性确证后, 无法将嵌入在图像中的水印信息移除, 换言之, 含水印图像在通过认证后, 无法还原成原始图像, 这是由于传统的水印嵌入技术会引入不可逆的失真. 可逆水印又称为无损水印或无失真水印, 它是指含水印图像在检测端被确证为真实无误后, 嵌入的水印信息可被完全抹除而恢复出原始图像.

目前已提出了多种可逆水印算法, 如: Hon-singer^[3]利用模 256 和的特点实现了空域可逆水印, 由于采用模 256 和的缘故, 所产生的水印图像可能会含有椒盐噪声. Fridrich^[4]使用无损压缩技术压缩空域像素的某些位平面以腾出空间来实现水印的可

逆嵌入. 为了能腾出较多的空间, 需要压缩像素的较高位平面, 这势必会降低含水印图像的质量. Ni 等^[5]通过选取图像灰度直方图的最高点并将之移位来实现水印的可逆嵌入. 上述这些算法均未考虑水印的安全性.

本文提出一种安全的用于图像认证的可逆水印算法. 算法使用参数化整数小波, 由参数控制小波基的选取, 如果嵌入参数与提取参数不一致, 水印信息将无法正确提取出来, 保证了水印的安全性, 此外利用细节子带整数小波系数的较高位平面能被有效压缩的特点^[6]实现了水印的可逆嵌入.

2 参数化整数小波变换

我们选用 CDF9-7 双正交小波, 对于一维信

收稿日期: 2009-07-09; 修回日期: 2009-09-09

基金项目: 国家自然科学基金项目(60873088, 60873198); 广东商学院校级科研一般项目(08YB52003)

号 $\{x_l\}_{l \in \mathbb{Z}}$, 根据文献[7] 和文献[8], 其基于提升格式的参数化整数小波变换构造如下:

$$\begin{cases} s_l^{(0)} = x_{2l} \\ d_l^{(0)} = x_{2l+1} \\ d_l^{(1)} = d_l^{(0)} + \text{Int}(\alpha(s_l^{(0)} + s_{l+1}^{(0)})) \\ s_l^{(1)} = s_l^{(0)} + \text{Int}(\beta(d_l^{(1)} + d_{l-1}^{(0)})) \end{cases} \quad (1)$$

$$\begin{cases} d_l^{(2)} = d_l^{(1)} + \text{Int}(\gamma(s_l^{(1)} + s_{l+1}^{(1)})) \\ s_l^{(2)} = s_l^{(1)} + \text{Int}(\delta(d_l^{(2)} + d_{l-1}^{(1)})) \end{cases} \quad (2)$$

$$\begin{cases} d_l^{(3)} = d_l^{(2)} + \text{Int}((\zeta - \zeta^2)s_l^{(2)}) \\ s_l^{(3)} = s_l^{(2)} + \text{Int}((-1/\zeta)d_l^{(3)}) \end{cases} \quad (3)$$

$$\begin{cases} d_l^{(4)} = d_l^{(3)} + \text{Int}((\zeta - 1)s_l^{(3)}) \\ s_l^{(4)} = s_l^{(3)} + d_l^{(4)} \end{cases} \quad \begin{cases} s_l = s_l^{(4)} \\ d_l = d_l^{(4)} \end{cases} \quad (4)$$

式中, s_l 和 d_l 分别为低频和低频分量, $s_l^{(i)}$ 及 $d_l^{(i)}$ ($i = 0, 1, 2$) 为中间结果, $\text{Int}(x)$ 为取整操作. 参数 α 、 β 、 γ 、 δ 、 ζ 这五个参数之间的相互关系见式(5).

$$\begin{cases} \beta = -\frac{1}{4(1+2\alpha)^2} \\ \gamma = \frac{-1-4\alpha-4\alpha^2}{1+4\alpha} \\ \delta = \frac{1}{16}(4 - \frac{2+4\alpha}{(1+2\alpha)^4} + \frac{1-8\alpha}{(1+2\alpha)^2}) \\ \zeta = \frac{2\sqrt{2}(1+2\alpha)}{1+4\alpha} \end{cases} \quad (5)$$

式中, α 的取值并非任意选取, 它的取值区间为 $(-3, -1.2)$ 内的实数^[7].

对于二维信号的参数化整数小波变换, 可先对行进行变换, 然后再对列变换得到小波变换图. 重构时则要先在列方向重构, 然后在行方向重构.

3 用于图像认证的安全可逆水印算法

图 1 和图 2 分别是水印嵌入和水印提取及篡改检测框图, 包括直方图修改、水印嵌入、水印提取及篡改检测和原始图像恢复等几部分. PIWT 代表参数化整数小波变换, IPIWT 表示参数化整数小波逆变换, 直方图修改的目的是为了防止因修改小波系数造成小波逆变换后图像像素溢出, 恢复原始图像是指待认证图像被证实为真实无误后, 使用隐藏在细节子带的信息还原出原始图像.

3.1 图像预处理

将信息嵌入到位于细节子带的小波系数的较高位平面, 逆变换之后, 有可能会使图像的像素溢出, 从而影响图像认证的结果. 为了避免像素溢出, 需对

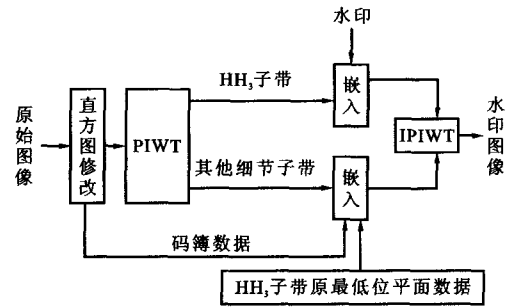


图 1 水印嵌入框图

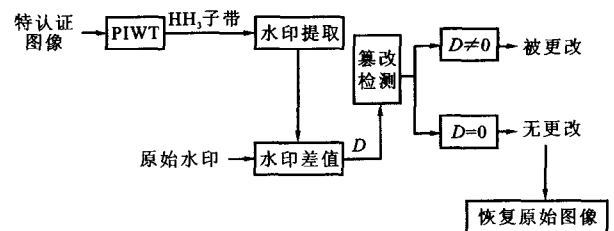


图 2 水印提取及篡改检测框图

原始图像进行预处理, 可以采用图像灰度直方图修改, 详见式(6).

$$I' = \begin{cases} \Delta & 0 \leq I \leq \Delta \\ 255 - \Delta & 255 - \Delta \leq I \leq 255 \end{cases} \quad (6)$$

式中, I 表示原始图像像素值, I' 是预处理后的图像像素值, Δ 可取 $[0, 30]$ 之间的整数, 本文 Δ 取 15.

这里记原始图像为 I_O , 预处理后所得到的图像记为 I_{HM} , 用 B 表示被修改了的灰度的原始信息.

3.2 水印嵌入

(1) 对经过预处理后的图像 I_{HM} 进行三级参数化整数小波分解, 记欲嵌入的水印信息为 W 及 HH_3 子带小波系数的 LSB(最低有效位) 位平面信息为 L , 将 W 替换 L 实现水印的嵌入;

(2) 采用算术编码无损压缩 HH_1 、 LH_1 、 HL_1 子带小波系数的第四个位平面, 记压缩后的数据为 C ;

(3) 将 B 、 C 、 L 三类信息组合成一个大的位串并替换 HH_1 、 LH_1 、 HL_1 子带小波系数的第四个位平面;

(4) 最后进行参数化整数小波逆变换, 得到含水印的图像.

3.3 篡改检测

记待认证的图像为 I_s , 将 I_s 进行三级参数化整数小波分解, 提取位于 HH_3 子带小波系数 LSB 位平面的水印信息, 记其为 W' , 依式(7) 计算水印差值图.

$$D = |W - W'| \quad (7)$$

式中, 水印差值图 D 反映原始水印与提取出的水印二者之间的差异. 若 D 中某点的像素值为 1, 则表明

该点被更改了,用白点表示.若 D 中某点的像素值为0,则表明该点没被更改过,用黑点表示.借助水印差值图,我们可以判断图像是否被更改,进而定位篡改区域.

3.4 图像恢复

当待认证的图像被证实为真实无误后,即可进行原始图像的恢复操作,步骤如下:

(1) 对图像进行三级参数化整数小波分解,由细节子带整数小波系数的第四个位平面提取隐藏信息 B 、 C 、 L ;

(2) 用 L 恢复 HH_3 子带的LSB位平面的原始信息, C 经解压缩用于恢复 HH_1 、 LH_1 、 HL_1 子带小波系数的第四个位平面的原始信息;

(3) 经三级参数化整数小波逆变换,得到直方图修改后的图像 I_{HM} ;

(4) 利用 B 将 I_{HM} 恢复为原始图像 I_O .

4 实验结果

采用 $512 \times 512 \times 8$ 的Baboon标准图像测试本文提出算法的性能,嵌入的水印为 64×64 的“广东商学院”二值图像,嵌入参数 $\alpha = -1.5$.

4.1 不可见性实验

图3(a)为原始图像,图3(b)为利用本算法得到的水印图像,其PSNR(峰值信噪比)为37.88dB,对比两幅图像,可见水印图像与原始图像在视觉上察觉不出差异,说明算法的不可见性好.

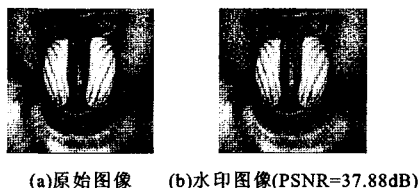


图3 水印不可见性

4.2 安全性实验

对使用嵌入参数为产生的水印图像,分别采用提取参数 $\alpha = -1.5$ 和提取参数 $\alpha' = -1.500\ 000\ 000\ 000\ 001$ 进行提取,所得结果见图4(a)及图4(b).由实验结果可以看出当提取参数与嵌入参数相同时,可以提取出正确的水印,而当嵌入参数与提取参数不同时,尽管两个参数相差低至 10^{-15} ,所提取出的水印是杂乱无章的.由于在 $(-3, -1.2)$ 之间可供选择的嵌入参数很多,所以只要攻击者不知道正确的嵌入参数,试图通过穷尽搜索参数来恢复水印信息的努力都是枉费心机的,可见本文提出的水印算法具有很高的安全性.

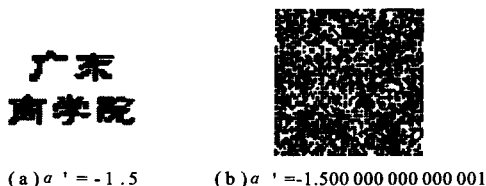


图4 不同提取参数的水印提取图

4.3 图像内容篡改实验

图5(a)是含水印的Baboon图像遭受剪切攻击后的图像,图5(b)为其水印差值图,可见水印差值图准确地定位出水印图像被篡改的区域.



图5 篡改检测图

5 结束语

本文提出一种用于图像认证的安全可逆水印算法,算法具有以下3个特点:(1)采用参数化整数小波变换,选择不同的嵌入参数相当于使用不同的小波基,从而提高了水印算法的安全性;(2)利用位于细节子带的整数小波系数较高位平面能够被有效压缩的特点,实现了水印的可逆嵌入;(3)生成的水印图像不可见性好,并且对图像被更改的区域能够实现准确定位.

参考文献:

- [1] 汪烈军,张太镒,李小和.基于图像内容的半易损水印认证算法[J].微电子学与计算机,2007,24(2):139-146.
- [2] 马刚,蒋志新,卫红春,等.一种基于LSB的易碎性数字盲水印算法[J].微电子学与计算机,2008,25(8):205-208.
- [3] Honsinger C W, Jones P, Rabbani M, et al. Lossless recovery of an original image containing embedded data[P]. US Patent:6 278 791, 2001.
- [4] Fridrich J, Goljan M, Du R. Invertible authentication[J]. SPIE Security and Watermarking of Multimedia Contents III, 2001(4314):197-208.
- [5] Ni Z, Shi Y, Ansari N, et al. Reversible data hiding[J]. IEEE International Symposium on Circuits and Systems, 2003(2):912-915.
- [6] Xuan G R, Zhu J, Chen J, et al. Distortionless data hiding based on integer wavelet transform[J]. IEE Electronics Letters, 2002, 38(25): 1646-1648.

(下转第44页)

位扩展加法器设计相比,电路面积接近,时序提高了 10%,总体性能较优.

分析新设计方法的电路面积,虽然采用的是 32 位的 SK 型加法器,比传统设计中 37 位的 SK 型加法器少了一级深度,但是由于对进位链的控制复杂,部分运算达不到满深度(例如,基于字节的运算只达到了深度 3,而满深度为 5),电路面积上出现冗余,所以电路面积上与传统设计接近,不存在优势.

分析新设计方法的关键路径,虽然增加了 3 个二选一选择器,但因为是在并行执行的,所以只增加了一级时延.同时,又因为加法结果和最高位进位不用提取,所以时序上较优.

6 结束语

通过与传统设计比较,可知该快速加法器的设计在维持电路面积基本不变的情况下,时序提高了 10%.如果设计对加法器的时序有严格的要求,则可以采用这种设计方法.

参考文献:

- [1] 庄伟.基于 AltiVec 技术的向量处理单元 VALU 设计与实现[D].西安:西北工业大学,2006:1-3.
- [2] 黄小平.支持 AltiVec 技术的可分裂式加法器研究与设计[J].计算机工程与应用,2009,45(12):63-65.
- [3] 靳战鹏.并行前缀加法器的研究与实现[J].微电子学与计算机,2005,22(12):92-95.
- [4] 胡铮浩.超前进位原理研究和逻辑设计改进[J].科技通报,1992,8(1):16-19.
- [5] Reto Zimmermann. Binary adder architectures for cell-based VLSI and their synthesis[D]. Flensburg: University of Rostock, 1997.

作者简介:

刘学政 男,(1983-),硕士研究生.研究方向为计算机系统结构、专用集成电路设计.

张盛兵 男,(1968-),教授,博士生导师.研究方向为 VLSI 系统设计、计算机系统结构、电子设计自动化.

黄小平 男,(1979-),博士研究生.研究方向为计算机系统结构、专用集成电路设计.

(上接第 39 页)

- [7] Daubechies I, Sweldens W. Factoring wavelet transforms into lifting steps[J]. Journal of Fourier Analysis, 1998, 4(3): 245-267.
- [8] Calderbank R, Daubechies I, Sweldens W, et al. Wavelet transforms that map integers to integers[J]. Journal of Applied and Computational Harmonic Analysis, 1998(5):332

- 369.

作者简介:

吴晓云 男,(1972-),博士,讲师.研究方向为多媒体信息安全、信息隐藏、数字水印.

胡建军 男,(1970-),博士,副教授.研究方向为商务智能、智能信息处理、数据库与知识工程.