基于整数小波变换的医学图像易碎水印方法

冯前进 陈凌剑 杨 丰
(南方医科大学医学生物医学工程学院,广州 510515)

摘 要 为了对医学图像进行快速鲁棒的认证提出了一种基于整数小波变换的易碎水印算法。该算法首先利用小波分解后的四叉树结构结合树节点上的统计信息和密钥来选择嵌入水印的位置,然后对确定嵌入水印的位置只嵌入 1bit 的水印信息。该算法具有以下特点:(1)图像嵌入水印后具有较高的信噪比,适用于医学图像的认证;(2)结合小波系数的统计信息来选择嵌入水印的位置,可保证水印的易碎性;(3)小波分解在空频域的特性使得算法对篡改有很强的定位能力;(4)可利用密钥对本算法进行保护,即使算法公开,也能抵挡恶意攻击。实验结果表明,该算法适用于医学图像的认证,并且复杂度较低,实用性较强。

关键词 整数小波变换 易碎水印 四叉树 密钥 定位
中图法分类号: TP309.2 **文献标识码**: A **文章编号**: 1006-8961(2006)05-0736-06

A Fragile Watermarking Scheme for Medical Images Based on Integral Wavelet Transform

FENG Qian-jin, CHEN Ling-jian, YANG Feng
(*Department of Biomedical Engineering, South Medical University, Guangzhou* 510515)

Abstract This paper presents a fragile watermarking scheme based on integral wavelet transform. The proposed method uses the Quadtrees structures received by the wavelet decomposition, statistical information on the nodes and secret key to choose the locations where to embed the watermarks. One bit watermark information will be embedded into the right location. The method has some characteristics: (1) it is adapts to medical images authentication due to the high Signal-to-Noise when the watermark embedded into images; (2) ensures the fragileness of watermark when it combines with the statistical information of wavelet coefficient to choose the locations where to embed the watermark; (3) it has a strong orientation ability for tampering because of the characteristics of wavelet decomposition in the spatial-frequency domain; (4) uses the secret key to protect the proposed method. It can resist the malice attack even if opening the method. The experimental result shows that the proposed method adapts to the medical images authentication, it is less complexity and more practicability.

Keywords integral wavelet transform, fragile watermark, quadtrees, secret key, orientation

1 引 言

随着医院管理数字化建设的推进,传统的医学图像保存、分发介质已由胶片转变为数字图像光盘、磁盘。这无疑为临床诊断带来了很多便利,但由于数字图像容易被修改,因此被分发的图像的认证就显得尤为重要。如今数字水印是一种常用的图像认证技术,可用于医学图像的认证。水印技术分为易碎水印和鲁棒水印两种,其中易碎水印是数字水印技术的重要分支。由于易碎水印强调的是对数据完整性和有效性的认证功能以及对数据破坏和攻击的

基金项目:国家自然科学基金重点项目(30130180);国家重点基础研究发展计划"973"项目(203CB716100);广东省科技计划项目(2003B30605)和国家科技攻关项目(2004BA706B01)支持
收稿日期:2005-10-14;**改回日期**:2005-11-11
第一作者简介:冯前进(1974~),男。2003 年获南方医科大学博士学位,现为南方医科大学副教授。主要研究医学图像处理。E-mail: kxm@fimmu.com

定位分析能力,因此特别适用于医学图像的认证。对易碎水印,通常从下列方面进行评价:(1)水印的不可见性,即对嵌入水印的图像,人眼不可能觉察到水印的存在,这就要求水印的嵌入尽可能小地改变原图像的信息,通常用峰值信噪比来衡量。这一点对于医学图像显得尤为重要;(2)水印的敏感性,即对篡改检测的敏感程度;(3)对篡改的定位能力;(4)水印检测时,不需要原始图像;(5)即使水印图像、算法完全公开,也能抵抗对水印的恶意攻击。

易碎水印技术一般可分为时域嵌入和变换域嵌入两种。目前已有多种易碎水印技术,但都存在一定不足。Walton 提出的检查和(Checksum)算法[1]首先计算每个像素字节的最高 7bit 的 Checksum 值(checksum 值定义为一系列固定长度的二进制序列的模 2 和),然后算法在图像中随机选取固定数目的像素,最后将每个像素的最低有效位(least significant bit, LSB)变成与对应的 Checksum 的比特位相同,以完成水印的嵌入。这样,图像认证时,只需检测图像的 Checksum 值与提取的水印信息是否一致即可。这种方法虽简单易行,但如果图像被篡改,则该算法只能给出图像已被改动的信息,却不能指示图像的改动位置。

Yeung 和 Mintzer 将一个二值图像作为水印嵌入到原始图像中[2],该算法是通过利用伪随机发生器对图像的每一个颜色通道生成一个查找表(look up table)来控制像素值的修改,水印嵌入完成后,再采用一个改进的误差扩散处理器将水印嵌入引起的视觉影响扩散开来,以进一步提高图像嵌入水印后的主观质量。这样图像认证时,就可根据提取的二值水印图像是否完整来判断被测图像的真伪。该算法简单快速,易于硬件实现,是至今被研究较多的一种算法。但算法的安全性取决于查找表的破译难度,若所嵌入的二值图像为已知信息,则算法的安全性将大大降低[3],即使不知道二值水印图像,也可以采用拼贴方法(collage attack)对其进行有效攻击[4]。

Wong 提出取一个与原始图像大小相同的二值图像作为水印信息[5],该算法首先将原始图像与水印图像分成相同大小的对应块,然后对每个图像块进行操作,即根据由最低有效位置零后的像素值得到的 Hash 结果与水印信息进行异或操作,并把异或结果经私钥加密后嵌入在原始图像的最低有效位上。而在图像认证时,则将最低有效位经公钥解密后与最低有效位置零后的像素的 Hash 值进行异或操作,若被测图像未被更改,则异或操作将会得到完整的二值水印图像;否则,将会得到破损的水印图像。该算法将密码学中的公开秘钥(public key)体制引入到数字水印认证系统中,由于其使每一个图像接收者均可以进行认证检测,从而使水印认证系统更加实用化。

在研究过程中,作者认为,设计适用于医学图像的易碎水印算法的关键在于,在嵌入信息较少的情况下(确保图像的高信噪比),不仅能保持水印的敏感度,同时对篡改具有定位能力。所以实验中笔者首先将图像进行分块处理,然后在每一块中嵌入一定的信息,当其中一块的嵌入信息遭到篡改后,可以找到篡改发生的位置,即可对篡改进行定位。另外,每块中嵌入的信息还应尽量少,以得到较高的信噪比。为了保证水印的敏感性,可利用块内像素信息的统计特征来决定水印的嵌入位置,以使得图像对块中任一像素的修改都能在水印上有所体现。在水印算法完全公开的情况下,为了抵抗对水印的恶意攻击,可引入密钥系统,以便使攻击者在知道算法,但不知道密钥的情况下无法自行嵌入、提取、替换或修改水印。本文提出了一种在小波域嵌入水印的新方法,由于小波变换具有良好的空间-频率分解特性,且小波系数还可按四叉树形式进行组织,每一棵四叉树中的小波系数实际上对应于原图的一个矩形区域,因此在每一棵树上嵌入一定的水印信息,就可以对篡改定位。为了保证高信噪比,本文在一棵树上只嵌入 1bit 信息。为了保证水印的敏感性,水印信息应嵌入到高频系数上,因为小波的高频系数反映的是图像的细节变化。但对于一棵四叉树,其高频系数为 4^{l-1} 个(l 为分解层数),因此具体的嵌入位置应该怎么确定是关键。本文利用四叉树上系数的统计信息,结合密钥系统来决定最终的嵌入位置,并使水印有很高的敏感性。本文采用的小波变换为整数小波变换,因为只有整数小波变换才没有浮点运算,且在实际变换中真正是完全可逆的。对于图像信噪比要求很高医学图像认证这种算法最为合适。另外,本文方法中,对每棵树上只嵌入 1bit 水印信息,如果用浮点小波的话运算,则误差可能导致水印的检出错误。

2　小波提升的基本原理

小波变换的基本思想是利用信号间存在的相关

性来建立产生信号的一种稀疏表示。经典的小波变换是通过 Fourier 分析来建立时频分析。小波变换的提升格式认为,在信号的空间域,将对信号实施分裂、预测、更新 3 个步骤实现的信号频率分解称为信号的小波提升。

对原始信号(数据集)$\boldsymbol{S}_j(2^j)$,$j\in\mathbf{Z}^+$ 经小波变换为低分辨率子集 $\boldsymbol{S}_{j-1}$ 与细节子集 $\boldsymbol{d}_{j-1}$,其提升方法的实现分为以下 3 个步骤:

(1) 分裂(split)

将信号 $\boldsymbol{S}_j$ 分裂为两个较小的子集 $\boldsymbol{S}_{j-1}$ 与 $\boldsymbol{d}_{j-1}$。其最简单的分裂方法就是将信号 $\boldsymbol{S}_j$ 的两个子集相交或交为空集,即 $\boldsymbol{S}_j=\boldsymbol{S}_{j-1}\cup\boldsymbol{d}_{j-1}$,$\boldsymbol{S}_{j-1}\cap\boldsymbol{d}_{j-1}=\varnothing$。显然,这两者是高度相关的。在这里,本文将信号 $\boldsymbol{S}_j$ 分裂为奇、偶两个序列,即

$$\text{split}(\boldsymbol{S}_j)=(\boldsymbol{S}_{j-1},\boldsymbol{d}_{j-1}) \tag{1}$$

其中,split( )表示对集合进行分裂,$\boldsymbol{S}_{j-1}$ 和 $\boldsymbol{d}_{j-1}$ 分别表示分解后的偶序列和奇序列。

(2) 预测(predict)

用偶数序列可以内插奇数序列,即

$$\boldsymbol{d}_{j-1}=P(\boldsymbol{S}_{j-1}) \tag{2}$$

其中,预测算子 P 反映了数据相关的模型。当然,预测值与真实值是有误差的,这个误差体现了预测算子 P 的逼近程度,误差越小越好。

$$\boldsymbol{d}_{j-1}=\boldsymbol{d}_{j-1}-P(\boldsymbol{S}_{j-1}) \tag{3}$$

$\boldsymbol{d}_{j-1}$ 是预测值与真实值的偏离值。由于分裂时,数据是按照奇偶位置交替分割的,显然 $\boldsymbol{S}_{j-1}$ 与 $\boldsymbol{d}_{j-1}$ 的相关性最好,预测值也最有效。

继续分裂与预测

$$\{\boldsymbol{S}_{j-2},\boldsymbol{d}_{j-2}\},\boldsymbol{d}_{j-2}=\boldsymbol{d}_{j-2}-P(\boldsymbol{S}_{j-2}) \tag{4}$$

$$\{\boldsymbol{S}_{j-3},\boldsymbol{d}_{j-3}\},\boldsymbol{d}_{j-3}=\boldsymbol{d}_{j-3}-P(\boldsymbol{S}_{j-3}) \tag{5}$$

n 次分裂预测后,有

$$\boldsymbol{S}_j=\{\boldsymbol{S}_{j-n},\boldsymbol{d}_{j-n},\boldsymbol{d}_{j-n+1},\cdots,\boldsymbol{d}_{j-1}\} \tag{6}$$

(3) 更新(update)

实际上,由于预测一般不能保持原始信号 $\boldsymbol{S}_j$ 中的某些整体性质,如图像处理中要求子图像 $\boldsymbol{S}_{j-1}$ 要保持原有图像的亮度,即像素平均值不变。但分裂与预测继续到 $\boldsymbol{S}_{j-n}$ 仅含一个像素时,由于它是原图像中的任意像素值,而不是总体平均值,故需更新。更新过程就是找一个更好的 $\boldsymbol{S}_{j-1}$,其要能保留 $\boldsymbol{S}_j$ 的一些尺度特性 Q,即

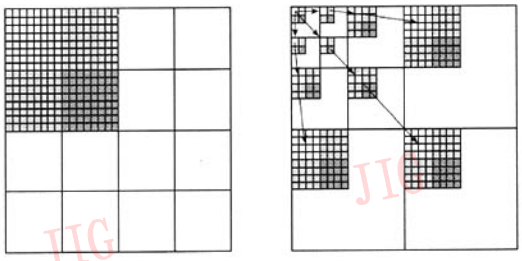
$$Q(\boldsymbol{S}_{j-1})=Q(\boldsymbol{S}_j) \tag{7}$$

为此可构造一个算子 U 去更新 $\boldsymbol{S}_{j-1}$,

$$\boldsymbol{S}_{j-1}=\boldsymbol{S}_{j-1}+U(\boldsymbol{d}_{j-1}) \tag{8}$$

3 算法概述

图像经小波分解后的系数可按树结构进行组织,称为空间小波树结构(如图 1 所示),其中低频分量 $\boldsymbol{LL}$ 中的系数为树根,其他高频分量中的系数为树枝和树叶。对于一个大小为 $M\times M$ 的图像,其低频分量 $\boldsymbol{LL}$ 大小为 $M^2/2^{2l}$,l 为小波分解的级数,即所有小波系数可以组织成 $M^2/2^{2l}$ 个小波树。由小波系数的空-频局部化特性可知,图 1(b)中的每棵空间小波树实质上定义了图 1(a)所示的一个原始图像块,每个原始图像块的大小为 2^{2l},其中 l 为分解的级数。



(a) (b)

图 1 空间小波树示意图

Fig. 1 Illustration of the wavelet tree

3.1 水印的嵌入过程

水印嵌入过程如图 2 所示。

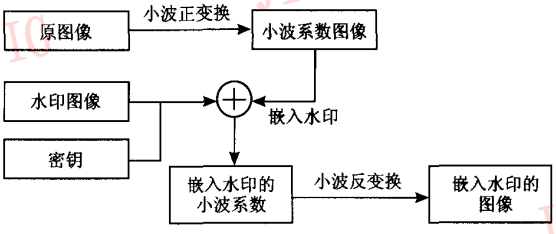


图 2 水印嵌入过程示意图

Fig. 2 Embedding processing

为了便于说明,先对以下符号进行说明:

$I(x,y)$ 表示低频(频带 $\boldsymbol{LL}$)小波系数,x,y 为其坐标,其在小波树中为树根;

$I^{(1)}_{HL,LH,HH}(x,y)$ 是以 $I(x,y)$ 为父节点的小波系数。

$I^{(2)}_{HL,LH,HH,LL}(x,y)$ 是以 $I^{(1)}_{HL,LH,HH}(x,y)$ 为父节点的小波系数。$I^{(2)}_{HL\,LH,HH,LL}(x,y)$ 的位置见图 3。

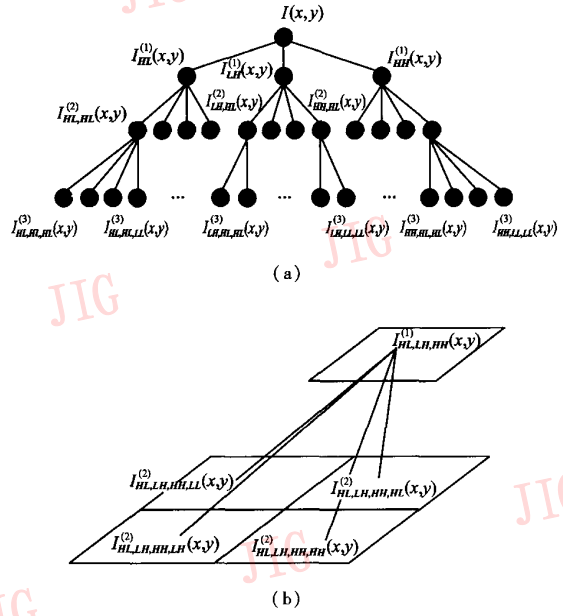


图 3　符号说明示意图

Fig. 3　Illustrations to symbols

$I^{(n)}_{HL,LH,HH,LL}(x,y)$,代表以 $I^{(n-1)}_{HL,LH,HH,LL}(x,y)$ 为父节点的小波系数。

若在每棵树中嵌入水印信息,则当图像遭到篡改后,只要检测到任意一棵树中的水印信息改变,就可实现对篡改的定位。其定位的精度随小波分解级数的增加、小波树数量的减少而减弱。为了保证嵌入水印的图像具有高信噪比,在每一棵树上嵌入的信息应越少越好,本文采用的方法是,如果只对每棵树上的一个节点进行修改,且只修改其最低有效位,则如何选择嵌入的节点是关键。本文节点的选择是基于以下考虑:(1)节点应位于最高频,因为最高频的系数反应的是图像的细节变化,其对于篡改会更敏感;(2)节点位置的选择要考虑小波树上系数的统计信息,以便使得树上任一节点的改变都能影响到节点位置的改变,这样水印的敏感度才高;(3)节点位置的选择要结合密钥进行,这样才能在算法公开的情况下抵抗恶意攻击。

设 $\boldsymbol{T}$ 是水印图像,大小为 $N\times N$,则

$$\boldsymbol{T}=\{w(m,n),w(m,n)\in\{0,1\},0<m,n<N\} \tag{9}$$

其中,$w(m,n)$ 表示水印图像像素在 (m,n) 处的灰度值。一般设水印的尺寸小于原始图像的尺寸,并且满足 $M=2^l\times N$。

水印嵌入过程的具体步骤如下:

(1)将原始图像 $\boldsymbol{I}$ 经过 3 级小波变换,得到不同分辨率下的细节子图 $I^{(1)}_{HL,LH,HH}(x,y)$ 和一个逼近子图 $I(x,y)$,$\hat{\boldsymbol{I}}$ 表示小波变换后的图像,$\boldsymbol{W}$ 表示离散小波变换。

$$\hat{\boldsymbol{I}}=\boldsymbol{WI} \tag{10}$$

其中,对图像信号(数据集)$\boldsymbol{S}_j, j\in\mathbf{Z}^+$,进行小波整数提升的过程如下:

①分裂,分裂过程是将原始数据集按奇、偶分裂为

$$\boldsymbol{S}_{j-1,k}=\boldsymbol{S}_{j,2k};\ \boldsymbol{d}_{j-1,k}=\boldsymbol{S}_{j,2k+1} \tag{11}$$

其中,$k=0,1,\cdots,2^{j-1}-1$;

②预测,对于奇数位置上的 $\boldsymbol{S}_{j,2k+1}$,是用相邻偶数 $\boldsymbol{S}_{j,2k}$ 与 $\boldsymbol{S}_{j,2k+2}$ 的线性平均去预测 $\boldsymbol{d}_{j-1,k}$ 的,也就是

$$\boldsymbol{d}_{j-1,k}=\boldsymbol{S}_{j,2k+1}-(\boldsymbol{S}_{j,2k}+\boldsymbol{S}_{j,2k+2})/2 \tag{12}$$

③更新,利用第 2 步预测后的相邻位置上的数值进行更新,这样可以保留 $\boldsymbol{S}_j$ 的一些尺度特性,即

$$\boldsymbol{S}_{j-1,k}=\boldsymbol{S}_{j,2k}+(\boldsymbol{d}_{j-1,k-1}+\boldsymbol{d}_{j-1,k})/4 \tag{13}$$

(2)生成密钥 $\boldsymbol{K}$,$\boldsymbol{K}$ 为一正整数随机序列。这里产生的密钥 $\boldsymbol{K}$ 将作为水印嵌入的参考标准。

(3)通过下面的方法找寻节点:

①已知 $I(x,y)$,即可确定 $I^{(1)}_{HL,LH,HH}(x,y)$:

$$I^{(1)}_{HL,LH,HH}(x,y)=\mathrm{mod}[(|I(x,y)|\times k),3] \tag{14}$$

②已知 $I^{(1)}_{HL,LH,HH}(x,y)$,即可确定 $I^{(2)}_{HL,LH,HH,LL}(x,y)$:

$$I^{(2)}_{HL,LH,HH,LL}(x,y)=\mathrm{mod}\left[\left(\sum_{HL,LH,HH}(|I^{(1)}(x,y)|)\right)\times k,4\right] \tag{15}$$

③依次类推,到最高频时,即可确定 $I^{(n)}_{HL,LH,HH,LL}$

$$I^{(n)}_{HL,LH,HH,LL}(x,y)=\mathrm{mod}\left[\left(\sum_{HL,LH,HH,LL}(|I^{(n-1)}_{HL,LH,HH,LL}(x,y)|\&0xfffffffe)\right)\times k,4\right] \tag{16}$$

上面的式子中 $\mathrm{mod}[a,b]$ 表示 a 除以 b 的余数;& 为按位与运算;k 为顺序从密钥序列中取出的一位密钥。

找到相应的节点后,就可根据水印图像的灰度值来替换该节点的最低有效位。如果 $w(m,n)=1$,则将节点最低有效位置 1;如果 $w(m,n)=0$,则将节点最低有效位置 0。

(4)对嵌入了水印的原始图像进行小波逆变换,就可以实现静态图像上水印的嵌入。$\hat{\boldsymbol{I}}_w$ 表示小波反变换后含水印的图像。

$$\hat{\boldsymbol{I}}_w = \boldsymbol{W}^{-1}\boldsymbol{I}_w = \{I_w(x,y), 0 < x,y < M\} \quad (17)$$

其中，$\boldsymbol{I}_w$ 表示嵌入了水印后的图像总像素点的集合；$\boldsymbol{W}^{-1}$ 表示逆离散小波变换；$I_w(x,y)$ 表示原始图像嵌入水印后在 (x,y) 处的灰度值。而对变换后的图像进行重构的过程，就是提升算法的逆过程。

$$S_{j,2k} = S_{j-1,k} - (d_{j-1,k-1}d_{j-1,k} + 2)/4 \quad (18)$$

$$S_{j,2k+1} = d_{j-1,k} + (S_{j,2k} + S_{j,2k+2})/2 \quad (19)$$

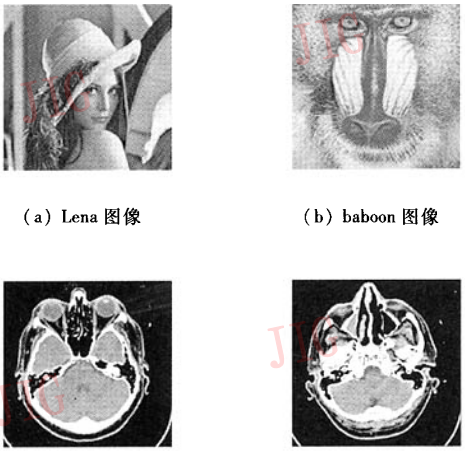
3.2 水印的提取

水印的提取过程是嵌入的逆过程。在提取水印时，并不需要用到原始图像。水印提取时，首先将含水印图像 $\boldsymbol{I}_w$ 进行 3 级小波变换，然后根据密钥 $\boldsymbol{K}$ 结合像素值所给出的顺序找到嵌入水印的位置，最后按照嵌入时的规则把水印提取出来。本文用峰值信噪比（peak signal noise ratio，PSNR）来对含水印图像 $\boldsymbol{I}_w$ 的扭曲程度进行客观评价，其定义为

$$PSNR = 10 \times \lg \frac{M^2 \times \max_{m,n} I^2(x,y)}{\sum_{m,n} (I(x,y) - I_w(x,y))^2} (\mathrm{dB}) \quad (20)$$

4 实验结果

为了验证本文算法效果，用本文算法对一组自然图像和一组医学图像（图 4）进行了水印嵌入实验，图像大小均为 512 × 512，原始水印图像和提取的水印如图 5 所示，大小为 64 × 64。实验中，用 Daubechies 5/3 滤波器（可逆）和基于 2 维离散小波变换（discrete wavelet transform，DWT）的提升算法来对图像做 3 级小波变换。



（a）Lena 图像　（b）baboon 图像

（c）CT1 图　（d）CT2 图

图 4 两幅自然图像和一组颅骨 CT 图像

Fig. 4 A group of natural image and phantom CT image

（a）原始水印　（b）提取的水印

图 5 原始水印与提取的水印

Fig. 5 Original watermark and extracted watermark

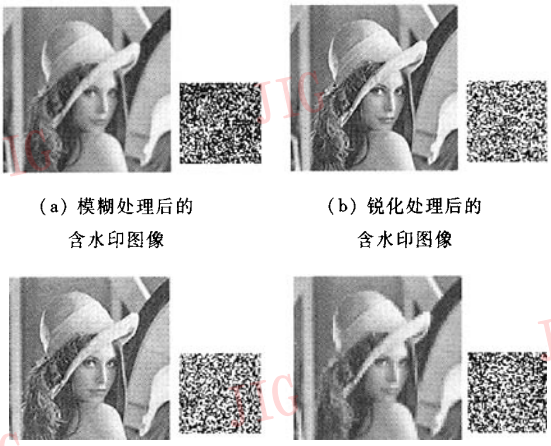
从表 1 可以看出，不管是自然图像还是医学图像，用本文算法嵌入水印后的图像都能具有很高的峰值信噪比，*PSNR* 都在 65dB 以上。这说明这种水印满足不可见性的要求，这一点对医学图像尤为重要。

表 1 图像嵌入水印后的峰值信噪比

Tab. 1 *PSNR* of the watermarked images

原始图像	Lena	baboon	CT1	CT2
PSNR(dB)	66.73	65.72	66.31	66.69

图 6 验证了本文方法对各种篡改的检测效果，其分别为对嵌入了水印的图像进行模糊、锐化、加入噪声、马赛克现象等篡改后的图像与提取出的水印图像。由图 6 可以看出，水印都被完全破坏了，这说明本文算法能够敏感地检测各种篡改，并可直观地将篡改反映出来。



（a）模糊处理后的含水印图像　（b）锐化处理后的含水印图像

（c）加入噪声后的含水印图像　（d）出现马赛克现象的含水印图像

图 6 本文方法对各种篡改的检测效果

Fig. 6 The authentication result of our method to every tampering test

图 7 验证了本方法对篡改的定位能力。实验中，对嵌入了水印的图像在 5 个不同的位置进行了

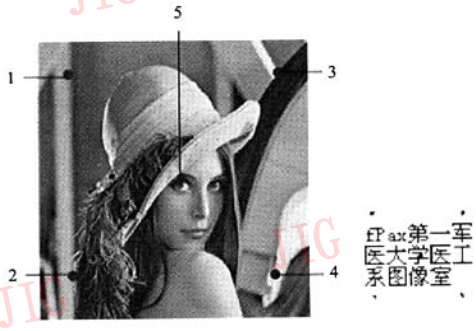


图 7　篡改定位实验

Fig. 7　Localization experiment

小面积的改动,由图 7 可见,在提取的水印的相应位置都遭到破坏,这证明了本方法有很强的定位能力。

5 结　论

本文提出了一种基于整数提升小波的易碎水印方案。该方案首先利用小波系数金字塔结构,按四叉树的形式组织小波系数,然后利用每棵树上的节点的统计信息,结合密钥来确定嵌入水印的位置。由于该算法对确定嵌入水印的位置只嵌入 1bit 的水印信息,因而保证了图像具有高信噪比,嵌入水印后的图像的峰值信噪比都在 65dB 以上,而目前作者所查找到的文献中的信噪比通常在 50dB 以下,这种高信噪比的特点特别适用于医学图像的认证,同时由于水印嵌入点的选择用到了小波系数的统计信息,因而保证了水印的易碎性。这一方面由于小波分解在空频域具有特有的分辨率,因而使本算法对篡改具有很强的定位能力;另一方面,由于算法引入了密钥,从而使得算法在完全公开的情况下,也能抵抗恶意攻击。综上所述,笔者认为,本文算法是一种适用于医学图像认证的易碎水印方案,很有应用前景。

参考文献(References)

1　Walton S. Information authentication for a slippery new age[J]. Dr. Dobbs Journal, 1995, **20**(4):18 ~ 26.

2　Yeung M Mintzer F. Invisible watermarking for image verification [J]. Journal of Electronic Imaging, 1998,7(3):578 ~ 591.

3　Memon N, Shende S, Wong P. On the security of the Yeung-Mintzer *authentication watermark*[A]. *In*: *Final Program and Proceedings of* the IS&T PICS'99[C], Savanna, Georgia USA, 1999:301 ~ 306.

4　Fridrich J, Goljan M, Memon N. Further attacks on Yeung-Mintzer fragile watermarking scheme[A]. In: Proceedings of SPIE[C], San Jose, CA, USA, 2000, **3971**:428 ~ 437.

5　Wong P W. A public key watermark for image verification and authentication [A]. In: Proceedings of the IEEE International Conference on Image Processing[C], Chicago, Illinois, USA, 1998, **1**:455 ~ 459.