基于 Hash函数敏感性的医学图像精确认证

钟晓燕 冯前进 陈武凡 江贵平
(南方医科大学生物医学工程学院, 广州 510515)

关键词 医学图像认证 易碎水印 整数小波变换 小波树 Hash函数
中图法分类号: TP309.2 **文献标识码**: A **文章编号**: 1006-8961(2008)02-0204-05

Hard Authentication for Medical Image Based on Sensitivity of Hash Function

ZHONG Xiao-yan, FENG Qian-jin, CHEN Wu-fan, JIANG Gui-ping
(Department of Biomedical Engineering, South Medical University, Guangzhou 510515)

Abstract A fragile watermark is designed using integral wavelet transform combined with hash function in order to verify the integrity of medical images. Even 1 bit of change in the picture can be sensed. Furthermore the region distorted can be easily oriented in this algorithm without an original image. Compared with the traditional digital watermark based on wavelet transform, the integer wavelets not only simplify the calculation but also improve the quality of watermarked image. And the hash function constructed with MD5 algorithm increases the security and ability of tamper localization of watermark. The results of experiment indicates that watermark scheme is highly sensitive to the distortion of the image. Since it requires a key during both the insertion and the extraction procedures, it has high security and the whole process is simple and accurate.

Keywords medical image authentication, fragile watermark, integral wavelet transform, quadtrees, Hash function

1 引 言

随着图像处理和计算机技术的不断进步和发展, 数字成像技术在医学中的应用日益广泛, 如它在医学超声成像技术、X-CT、MR及核医学成像中的应用等。另一方面以计算机网络为基础的图像存储和传输系统 PACS(picture archive and communication system)及其应用也在不断地发展。医学图像的数字化使得对医学数字图像的恶意篡改成为可能, 由此将造成较多的医疗纠纷, 因此在这个信息数字的时代如何对数字媒体内容的真实性和完整性实施有效保护已成为一个严峻的现实问题。对于大多数应用而言, 图像内容的微小改变可能都是可以接受的, 但是在医疗诊断时, 原有图像是否发生变化对于诊断结果就是非常重要的。因此在对医学图像进行真实性验证时, 应当采用精确认证, 即使用易碎水印。易碎水印算法大都由空间域 LSB水印算法演变而来。Walton首次提出用易碎数字水印的方法实现图像认证[1], Yeung利用一个密钥 K为每个基本色产生一个查询表 LUT(look up tables) 通过修改每个像素值使之恰等于对应的水印信息, 从而完成水印信息的嵌入, 从

基金项目: 国家自然科学基金重点项目(30730036); 国家重点基础研究发展计划 973项目(2003CB716104)
收稿日期: 2007-02-07; **改回日期**: 2007-07-02

第一作者简介: 钟晓燕(1977~), 女。现为南方医科大学医学信息研究所硕士研究生。主要研究方向为医学图像认证和编码等。E-mail: dawnswallow212@163.com
通讯作者: 江贵平, E-mail: gzjiang@263.net

而可以把篡改定位精确到一个像素[2]。Wong提出基于易碎水印的分块认证算法[3], 不久 Wong又将密码学中的公开密钥密码系统引入到水印信息加密中, 从而提高了原系统的安全性[4]。必须指出的是空间域方法的优点是能够嵌入较多的水印, 但难以定位频率篡改, 因为标记加在某些特定像素上, 常常不能检测对整幅图像的频率改动。

本文在 Wong的基础上提出了一种基于提升格式的整数小波变换和 Hash函数敏感性相结合的易碎水印方法。即首先应用整数提升小波变换, 然后构造出小波树结构, 利用小波变换系数的树结构关系和各层小波系数的特点在每棵小波树上嵌入一位水印信息。同时结合 MD5算法构造的 Hash函数和经典的密码学理论来设计水印算法, 以实现对医学图像的精确认证。由于这种易碎数字水印是将加密算法与图像处理技术相结合, 因此算法可完全公开, 使用者只要持有密钥, 就可以保证安全。实验结果表明, 本文提出的易碎水印算法不仅具有文献 [3] 所述的较好篡改敏感性, 而且具有比文献 [3]较好的峰值信噪比 PSNR(peak signal to noise ratio)。

2　基于整数小波变换的易碎水印算法

2.1　水印的嵌入

设 $\boldsymbol{W}$是二值水印图像, 大小为 $p \times p$, $W(u, v) \in \mathbf{Z}(u \in [0, 1) \wedge \mathbf{Z}, v \in [0, 1) \wedge \mathbf{Z})$, 其中 $W(u, v)$表示水印图像像素在 (u, v)处的灰度值。为了提高嵌入水印图像的质量, 采取在每颗小波树上嵌入一位水印信息

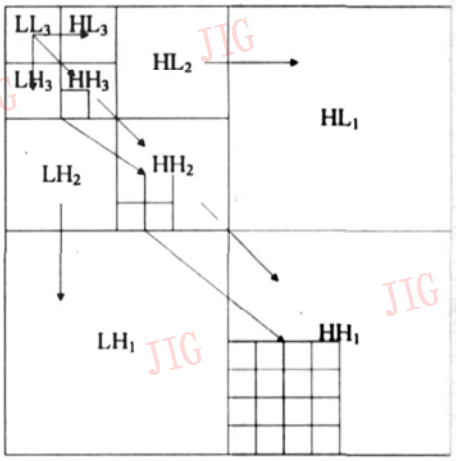
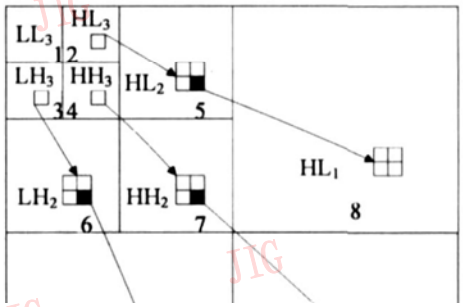


图 1　小波多分辨率分解

Fig. 1　Wavelet multi-resolution decomposition

小的区域来表示(如图 2所示)。第 1层小波变换系数的检测分辨率 2×2pixel/块, 第 2层小波变换系数的检测分辨率 4×4 pixel/块, 依次类推, L层小波系数的检测分辨率为 $2L \times 2L$ pixels/块。为了获得较高的定位精度和较好的图像质量, 将水印嵌入到第 1层的细节分量上。采用 3级小波分解, 因此篡改区域的定位精度为 8×8pixels/块。



轴 3×3个细节子图, 如图 1所示。升次基于提升框架的整数小波变换可以保证图像在进行小波变换和重构过程中不存在能量损失, 适用于医学图像这种感觉质量要求较高的数字水印领域。同时由于 DWT具有多分辨率特性, 使得算法可以检测到各个分辨率下篡改的特性, 从而定位篡改攻击的能力强。

(2) 小波树结构　小波变换 (DWT)后给出了图像在不同分辨率上的表示, 每个 DWT系数反映了图像在局部空域和局部频域上的内容。图像的 DWT系数具有一个 4分树结构, 即某一分辨率上的图像区域在更为精细的下一分辨率上被分成 4块较

(3) 密钥的生成　为了保证隐藏信息的安全, 构造出了基于 MD5算法的 Hash函数, 生成嵌入点密钥 E_K。

所谓 Hash函数, 要求满足:

已知 Hash函数的输出, 要求它的输入是困难的, 即已知 $c = \mathrm{Hash}(m)$, 求 m 是困难的。

已知 m, 计算 $\mathrm{Hash}(m)$是容易的。

已知 $c1 = \mathrm{Hash}(m)$, 构造 $m2$使得 $\mathrm{Hash}(m2) = c1$是困难的。

c= Hash(m), c的每一比特都与 m 的每一比特相关, 并有高度的敏感性。即每改变 m 的一比特, 都将对 c产生影响。

基于 MD5算法的 Hash函数是把输入任意长的消息, 以 512位输入数据块为处理单位, 且每一分组又被划分为 16个 32位子分组, 经过了一系列的处理后, 算法的输出由 4个 32位分组组成, 将这 4个 32位分组级联后将生成 128bits长的摘要, 发生相同摘要值的碰撞的几率为 $(1/2)^{128}$。从而保证当 MD5输入(如图 3所示的图像内容、图像 ID、密钥 K)发生任何微小变化时, 则生成的嵌入点密钥必然发生改变, 也就不能正确提取出水印。并且可以利用该函数的初值敏感性进行篡改定位, 定位是通过检测 Hash值所确定的嵌入位置提取出的信息来进行, Hash函数的高度敏感性使得篡改检测非常直观, 如果检测出来的水印图像是噪声图像, 则说明图像已经被篡改。

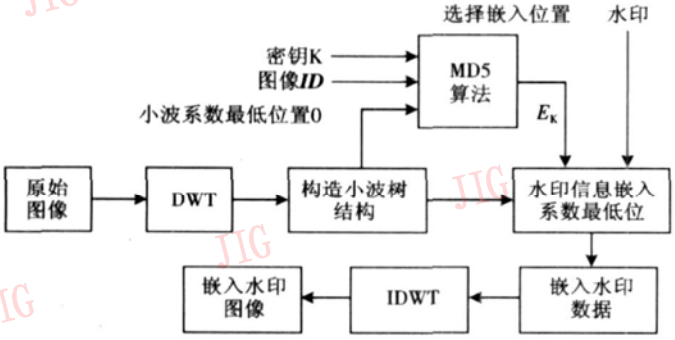


图 3 水印嵌入框图

Fig 3 The block diagram of watermarking embedding system

(4) 定位嵌入点

取根节点为 $LL_3(1, 1)$的这棵小波树 $tree(LL_3(1, 1))$; 将属于 $tree(LL_3(1, 1))$上的所有节点值 LSB置 0, 得到 $tree'(LL_3(1, 1))$。

以 $tree'(LL_3(1, 1))$和图像 ID、密钥一起作为 MD5的输入, 得到$H(tree'(LL_3(1, 1)))$, 记为 E_K, 以它作为水印嵌入的密钥, 每次循环左移两位, 取低两位确定嵌入位置的走向, 最终定位于相应的叶节点处, 嵌入水印信息。

如图 4所示, 如果用 key表示取出的低两位信息。

当处于根节点时:

$$\begin{cases} key = 00, \text{则定位于 } x_0^{(i,j)} \\ key = 01, \text{则定位于 } x_1^{(i,j)} \\ key = 10、11, \text{则定位于 } x_2^{(i,j)} \end{cases} \quad (1)$$

当处于叶节点时:

$$\begin{cases} key = 00, \text{则定位于 } x_{r\,0}^{(i,j)} \\ key = 01, \text{则定位于 } x_{r\,1}^{(i,j)} \\ key = 10, \text{则定位于 } x_{r\,2}^{(i,j)} \\ key = 11, \text{则定位于 } x_{r\,3}^{(i,j)} \end{cases} \quad (2)$$

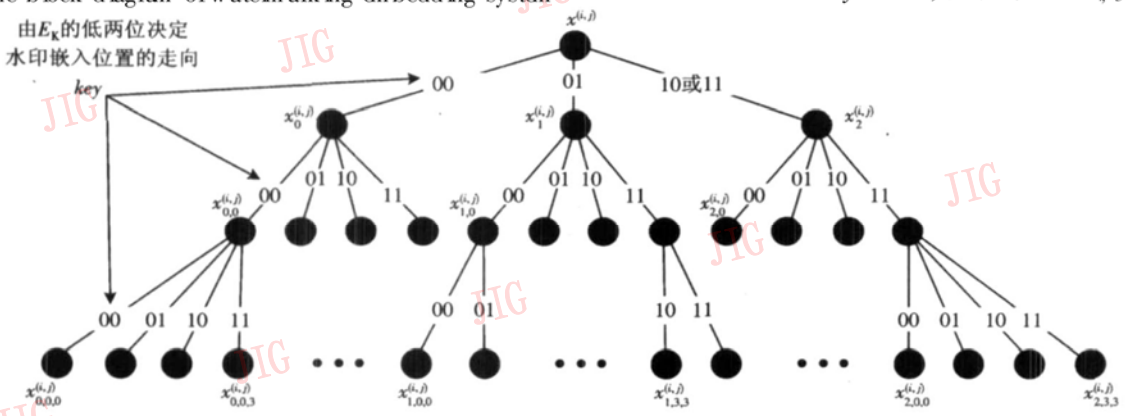


图 4 水印嵌入位置选择

Fig 4 Choose embedded position of watermarking

(5) 嵌入运算 为了提高水印敏感性, 在嵌入脆弱水印的过程中, 是采用嵌入小波系数最低位的方法来嵌入水印, 即对每棵树上的相应位置的小波系数嵌入一位的水印信息。嵌入规则如下: $W(i)$为第 i位的水印信息, 取 0或 1, 如果值为 0, 则将相应节点最低有效位置 0, 反之, 置 1。重复至所有的小波树都已经嵌入水印信息。

(6)对嵌入了水印的小波系数进行小波逆变换, 得到嵌入水印图像。嵌入算法的基本框图如图 3所示。

2.2 水印的提取

水印的提取是嵌入的逆过程。检测水印时, 首先对水印图像进行 3级小波分解, 按小波树形式组织小波系数, 按照嵌入的过程寻找到嵌入点提取出水印信息。

$$\begin{cases} \widetilde{W}(i) = 0 & \widetilde{W}_F(x_i, y_i) \bmod 2 = 0 \\ \widetilde{W}(i) = 1 & \widetilde{W}_F(x_i, y_i) \bmod 2 = 1 \end{cases} \quad (3)$$

式中, $\tilde{W}_F(x_i, y_i)$ 为嵌入水印后图像在点 (x_i, y_i) 处的小波变换系数, mod表示取余, $\tilde{W}(i)$ 为提取出的第 i 位的水印信息。可见水印抽取并不需要原始图像, 从而实现了所谓的不需要原始图像的盲检 (blind detect)算法。

3　实验结果与分析

(1) 水印不可见性实验

以一幅 512×512的 256级灰度图像 Lena为例做模拟实验, 算法采用 Daubechies5/3滤波器 (可逆)和基于 2维离散小波变换 (DWT), 嵌入一幅 64×64的二值图像。对图像的质量采用峰值信噪比 (PSNR)来进行评价。

$$\mathrm{PSNR} = 10\lg\frac{M^2 \times \max_{m,n} x^2(m, n)}{\sum_{m,n}(x(m, n) - x'(m, n))^2} \quad (4)$$

图 5演示了标准图 Lena和医学 CT图像嵌入和提取水印的实验。其中嵌入水印后的 Lena图像和医学 CT图像的 PSNR分别为 65.2dB和 65.5dB, 可见这种易碎水印不仅满足不可见性的要求, 而且具有较高的峰值信噪比, 适用于医学图像认证。

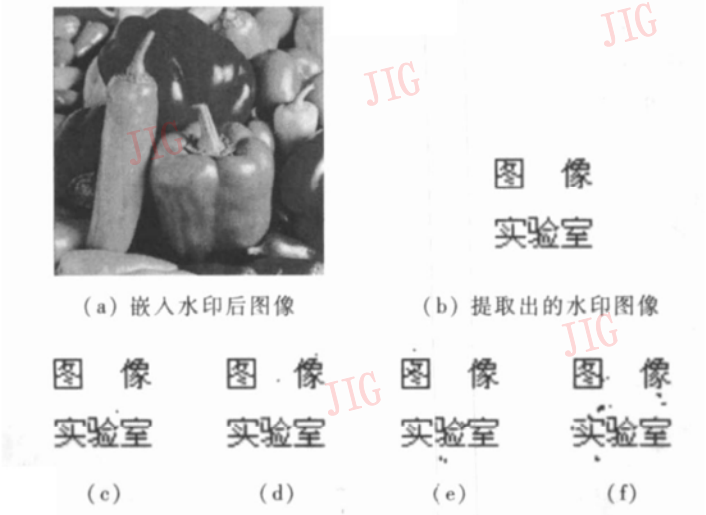
(a) 水印图像　(b) 原始 Lena 图像　(c) 嵌入水印后的图像　(d) 原始 CT 图像　(e) 嵌入水印后的 CT 图像

图 5　水印不可见性实验

Fig. 5　Invisibility experiments of watermarking

(2) 敏感性实验

通过图 6的实验来验证水印对篡改的敏感性。图 6(c) ~ (f)分别为图 6(a)中水印图像随机的选择位置和幅度其一、二、五、十个像素点篡改以后的图像中相应提取出来的水印图像。由此可见, 这种易碎水印对篡改极度敏感, 可以检测到图像 1bit的篡改并且可直观地将篡改反映出来。这种敏感性主要来源于 Hash函数对输入的强相关性, 即输出的每一比特都与输入的每一比特相关, 以及对输入的高度敏感性, 即每改变输入一比特, 都将对输出值产生明显影响, 实验中常以雪崩性描述该性质: 输入改变任一比特, 输出的每一比特都以 1/2的概率改变。



(a) 嵌入水印后图像　(b) 提取出的水印图像

(c)　(d)　(e)　(f)

图 6　水印对图像篡改的敏感性实验

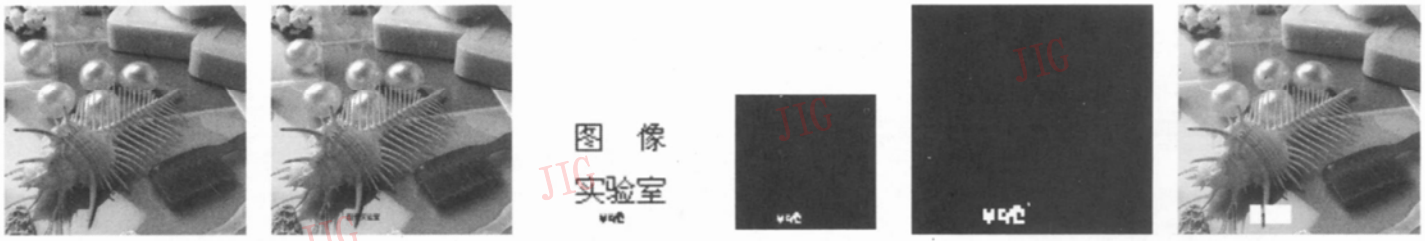
Fig. 6　Sensitivity experiments of watermarking towards tampered image

(3) 篡改定位实验

按照与水印嵌入相同的方法在相应的位置提取出水印, 与原始水印进行比较, 可进行篡改的检测与定位。为了使得认证算法具有一定的定位能力, 往往需要将宿主图像分割为独立的子块。显然图像子块尺寸越小, 定位的精度越高, 但计算量却越大, 所以需在定位精度和计算量之间进行折衷。这里选择 3级小波分解, 由小波树的结构分析相当于定位 8×8的块。图 7是易碎水印对篡改区域定位的实验结果。嵌入水印后的图 7(a), 经过篡改变为图 7(b)。从图 7(c)可以看出该方法能有效地检测到图像被篡改了, 图 7(f)中白色的图像域代表篡改区域。

(4) 对比实验

为了验证本文算法的有效性, 将本文算法与文献[3]、[8]做了比较, 如表 1所示。用篡改评估函数 TAF(tamper assessment function)来对比 3种算法对篡改的敏感性。



(a) 嵌入水印后的图像 (b) 水印图像添加文字后 (c) 提取出的水印 (d) 与原水印的差图 (e) 差图放大 8 倍 (f) 篡改区域定位

图 7 篡改区域定位试验

Fig. 7 Orientation experiment of tampered region

表 1 与其他算法的敏感性比较

Tab 1 Sensitivity comparison with other algorithms

算法	嵌入水印后 PSNR (dB)	各种攻击方式 (测试图像为 peppers)					
		椒盐噪声	高通滤波	锐化	旋转	压缩	剪切
本文算法	65.4	0.501	0.632	0.502	0.613	0.584	0.013
文献[3]中算法	51.1	0.353	0.500	0.498	0.498	0.499	0.006
文献[8]中算法	65.3	0.486	0.629	0.501	0.598	0.553	0.011

$$TAF = TAF(\omega, \overline{\omega}) = \frac{1}{N_l}\sum_{i=0}^{N_l}\omega_i \oplus \overline{\omega}_i \qquad (5)$$

式中, ω为原始水印序列, $\overline{\omega}$为提取水印序列, $\oplus$代表异或操作, N_l为水印的长度。

对水印图像进行加扰处理, 包括噪声、滤波、锐化、旋转、压缩、剪切等, 表 1给出了不同干扰, 水印图像的篡改评估值。由比较可知, 在各种干扰下本文算法的篡改评估值较文献[3]、[8]均有不同程度的提高, 即表明本文提出的易碎水印算法的篡改敏感性要优于文献[3]、[8], 同时本文算法的 PSNR 也高于文献[3]、[8]的算法, 从而可以进一步地提高嵌入水印图像的质量。

4 结 论

本文提出了一种基于整数小波变换、结合小波树结构和 Hash函数的易碎水印算法。整数小波变换能够在图像分解和重构过程中, 使得图像损失为零, 可提高水印图像质量。在小波树结构上嵌入水印信息, 可在时频域上定位篡改的区域。而 MD5算法构造的 Hash函数的运用提高了水印安全性和水印检测的能力。实验结果表明, 本文算法对篡改具有高度敏感性, 且整个认证过程还需密钥完成检测, 安全性很高, 认证过程计算简单且准确性很高, 是一种医学图像鉴定的有效方法。

参考文献 (References)

1 Walton S. Information authentication for a slippery new age[J]. Doctor 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 Wong P W, Memon N. Secret and public key image watermarking schemes for image authentication and ownership verification [J]. IEEE Transactions on Image Processing, 2001, **10**(10): 593~601.

4 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, USA, 1998: 455~459.

5 Lin E T, Delp E J. A review of fragile image watermarks[A]. In: Proceedings of the Multimedia and Security Workshop (ACM Multimeda'99) Multimedia Contents[C], Orlando, FL, USA, 1999: 25~29.

6 Coatrieux G, Maître H, Sankur B, *et al*. Relevance of watermarking in medical imaging[A]. In: IEEE-embs Information Technology Applications in Biomedicine[C], Arlington, USA, 2000: 250~255.

7 Wu Jin-hai, Lin Fu-zong. Image authentication based on digital watermarking[J]. Chinese Journal of Computers, 2004, **27**(9): 1153~1161. [吴金海, 林福宗. 基于数字水印的图像认证技术[J]. 计算机学报, 2004, **27**(9): 1153~1161.]

8 Feng Qian-jin, Chen Ling-jian, Yang Feng. A fragile watermarking scheme for medical images based on integral wavelet transform[J]. Journal of Image and Graphics, 2006, **11**(5): 736~741. [冯前进, 陈凌剑, 杨丰. 基于整数小波变换的医学图像易碎水印方法[J]. 中国图象图形学报, 2006, **11**(5): 736~741.]