一种基于整数小波变换的医学图像半脆弱水印算法*)

王 斌[1,3] 韩国强[1] 陈薇娜[2] 秦 拯[2,3]

(华南理工大学计算机学院 广州 510641)[1] (湖南大学软件学院 长沙 410082)[2]

(东莞理工学院软件学院 东莞 523808)[3]

摘 要 提出一种应用于医学图像的半脆弱水印算法。首先对RGB图像进行可逆颜色转换,再对亮度分量进行一维整数harr小波变换,然后通过自适应地修改高频系数以嵌入水印。实验表明,该算法具有较高的透明性,对非恶意攻击具有一定鲁棒性,同时能较好地对恶意攻击进行检测与定位,能方便地应用于医学图像管理与保护。

关键词 数字水印,半脆弱水印,整数小波变换,医学图像

A Semi-fragile Watermarking Algorithm Based on Integer Wavelet Transform for Medical Images

WANG Bin[1,3] HAN Guo-Qiang[1] CHEN Wei-Na[2] QIN Zheng[2,3]

(College of Computer Science and Technology, South China Univ. of Technologye, Guangzhou 510641)[1]

(Software College of Hunan University, Changsha 410082)[2] (Software College of Dongguan University of Technology, Dongguang 523808)[3]

Abstract A semi-fragile watermarking algorithm for medical images is proposed in this paper. Firstly, the RGB image is mapped to YUV image by using invertible color transform. Secondly, 1-D integer harr wavelet transform is applied to luminance Y. Thirdly, the watermark is embedded into the host image by modifying the detailed coefficients adaptively. The experimental results prove the high transparency and the good robustness to non-malicious attacks. At the same time, the scheme can locate the tampered region accurately. It can be applied on some medical image application domain for the copyright and management of medical images.

Keywords Digital watermarking, Semi-fragile watermarking, Integer wavelet transform, Medical images

1 引言

医学图像已经广泛地应用于临床活动的整个过程,常用医学图像主要包括:X光图像、超声图像、内窥镜图像、显微图片、断层及核磁共振图片。医生在工作中需要了解病人在各个部门检查的结果和临床的观察、治疗记录,以全面掌握病情。图像信息只是其中的一项检查结果,因此往往需要将这些信息与检查过程中的文字报告以及其他部门的检验结果、治疗记录、病程记录等信息相结合。传统的医学图像管理系统将图像信息和检查过程中的文字报告、其他部门检验结果、治疗记录、病程记录等信息分开存储,增加了医学图像管理的复杂性,同时也容易造成病人信息泄密。而数字水印的出现为医学图像管理提供了一种方便而安全的途径,可以保证病历的秘密性及与诊断依据之间的数据一致性[1]。数字水印是将包括病人和医生姓名、编号、检查日期时间、病变类型、病历片段等重要信息以水印形式隐藏在医学图像中,在病历与医疗图像间建立起一一对应关系,保持诊断数据的一致性,有利于方便快捷的检索。既能防止发生遗失错乱现象又能保证病历的秘密性,有效保护病人的隐私;另外,也可以嵌入自己特定的水印,为追踪泄密渠道提供手段。鉴于医学图像的特殊应用,与普通图像相比,医学图像对水印嵌入有一些独特的要求[1,2]:(1)由于医学图片的特殊性,它要求在加入水印时,对图片的改动很小;特别对一些关键部分(如病区)则不允许改动,即具有高透明性。(2)对所嵌入水印信息安全性有严格要求,尤其是某些特殊病人的病历为国家和企业机密,绝对不允许泄露,因此水印不能被非法提取。(3)作为水印的病历信息应该在需要时能被完整准确地提取出来,即嵌入水印具有一定鲁棒性。

Goljan提出一种可逆数据隐藏方法[3],其基本思想是将原始图像中用于嵌入数据的特征进行压缩,将压缩了的特征和待嵌入数据一起嵌入在原始图像中,能够嵌入的数据量是特征压缩后的冗余。在数据检测过程中,由于能够检测到原始图像特征,从而可以恢复原始图像。这种方法并不是指图像在嵌入过程中不产生任何失真,而是指这种失真是可逆的,但这同时破坏了隐藏信息与原始媒体的不可分离性,一旦隐藏数据从图像中提取出来,得到的无失真图像中就不再存在有隐藏数据。黄夏菱等针对调色板图像提出一种真正无失真隐藏算法[1],但隐藏后图像的调色板有一定规律(调色板前半部分与后半部分完全一样),很容易引起攻击者的怀疑。Honsinger等采用模数运算提出一种可逆的易损认证方法[4],但该方法易产生"椒盐"噪声。冯前进等提出一种基于整数小波的医学图像易损水印算法[2],但该算法是纯脆弱水印算法,不能抵抗非恶意攻击,实用性不强。

针对以上问题,同时考虑到整数小波变换具有良好的时频局部特性,与新的压缩标准JPEG2000相兼容,与人类视觉屏蔽特性相一致,不引入量化误差等优点,本文提出了一种高

*)资助项目:国家自然科学基金项目(No. 60573019),广东省科技计划项目(编号:2004B16001006),湖南省科技计划项目(编号:2006FJ4110),东莞市科研发展基金项目(No. 2004D1015,2005D025,2005D049)。王 斌 博士生,高级工程师,主要研究方向为多媒体信息安全、数字水印、图像处理等;陈薇娜 硕士研究生,主要研究方向为信息安全、数字水印。

透明性医学图像半脆弱认证水印算法。该算法保证了隐藏信息与原始媒体的不可分离性，在对非恶意攻击具有一定鲁棒性的同时具有一定的篡改检测与定位能力。

2 整数 Harr 小波

Harr 基小波函数定义在区间[0,1)上，见式(1)。对于 t 的平移，Harr 小波是正交的。对于一维 Harr 小波可以看成是完成了差分运算。

$$\psi_H(t)=\begin{cases}1, & 0\leqslant t<\frac{1}{2}\\ -1, & \frac{1}{2}\leqslant t<1\\ 0, & \text{其他}\end{cases} \tag{1}$$

设 x、y 为同一行相邻两个像素点的灰度值，满足：$0\leqslant x,y\leqslant 225$；记 x,y 均值为 s，差值为 d，则有：

$$s=\left\lfloor\frac{x+y}{2}\right\rfloor, d=x-y \tag{2}$$

则由式(2)可知整数 x,y 经过变换后得到的 s,d 均为整数，且

$$x=s+\left\lfloor\frac{d+1}{2}\right\rfloor, y=s-\left\lfloor\frac{d}{2}\right\rfloor \tag{3}$$

其中 $\lfloor\cdot\rfloor$ 表示向下取整数。则 s,d 分别为图像经过一维行变换后的低频和高频系数。

3 本文提出算法

3.1 水印预处理

设水印图像可表示为：

$$W_1=\{w_1(i,j)\mid 0<i\leqslant m,0<j\leqslant n,w_1(i,j)\in\{0,1\}\}$$

其中 m，n 分别为图像的宽度和高度。为了增强水印系统的安全性，在水印嵌入前先由密钥控制的置乱加密算法[6]对 w_1 进行置换之后得到最终待嵌入水印信号

$$W_2=\{w_2(i,j)\mid 0<i\leqslant m,0<j\leqslant n,w_2(i,j)\in\{0,1\}\}$$

3.2 水印嵌入

水印嵌入基本思想是：首先采用可逆颜色变换将 RGB 图像转换到 YUV 空间，以解除各颜色分量间的相关性，然后对亮度分量 Y 进行一维整数 Harr 小波变换，最后对高频系数进行自适应修改以嵌入水印。水印嵌入基本流程如图 1 所示。

本文采用的可逆颜色变换[5]的正变换为：

$$\begin{aligned}Y_r&=\left\lfloor\frac{R+2G+B}{4}\right\rfloor\\ U_r&=R-G\\ V_r&=B-G\end{aligned} \tag{4}$$

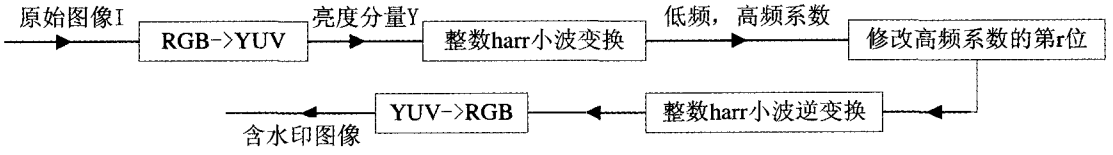


图 1 水印嵌入框图

其反变换公式为：

$$\begin{aligned}G&=Y_r-\left\lfloor\frac{U_r+V_r}{4}\right\rfloor\\ R&=U_r+G\\ B&=V_r+G\end{aligned} \tag{5}$$

具体嵌入过程如下：

首先输入 RGB 图像 I，运用公式(4)将图像 I 转换到 YUV 空间。

然后对亮度分量 Y_r 进行一维整数小波变换得到低频系数 s 和高频系数 d，于是我们可以通过自适应地修改高频系数 d 的第 r 位比特以嵌入水印。

$$r=\lfloor\alpha\times\lceil\log_2^d\rceil\rfloor \tag{6}$$

其中 $\lceil\cdot\rceil$ 表示向上取整，$\lfloor\cdot\rfloor$ 表示四舍五入，且有 $0<\alpha<1$，α 越大，水印的鲁棒性越好，反之则透明性越好。对第 r 位的修改规则为：若水印序列对应比特位为 1 则第 r 位置 1，若水印序列对应比特位为 0 则第 r 位置 0。这种嵌入规则使得高频系数越大，修改越大，而高频系数对应噪声和高频信息，人眼对这些信息相对不敏感，所以该嵌入方法在一定程度上考虑了人类视觉系统屏蔽特性，有助于水印算法的鲁棒性与透明性的提高；

之后再利用公式(3)进行一维逆 Harr 小波变换得到隐藏了水印的亮度分量 Y，最后由公式(5)将图像从 YUV 空间映射到 RGB 空间，即得到嵌入水印后图像。

3.3 水印提取

水印的提取过程基本上是嵌入过程的逆过程。首先用公式(4)将含水印的 RGB 图像转换到 YUV 空间，再对亮度分量 Y 进行一维整数 Harr 小波变换。由于水印嵌入不会引起相应高频系数比特位数发生改变，所以水印提取时同样可用式(6)计算出水印嵌入的比特位 r，这样只要直接提取第 r 位比特值就可得到水印信号

$$W_2'=\{w_2'(i,j)\mid 0<i\leqslant m,0<j\leqslant n,w_2'(i,j)\in\{0,1\}\}。$$

所得到的水印图像 W_2' 经过一个反置乱算法即可得到原始的水印图像 W_1'。

3.4 图像认证

我们称水印嵌入前后两图像之差为水印差图，其定义为

$$E=\left\{e(i,j)\,\middle|\,\begin{matrix}e(i,j)=|w_1(i,j)-w_1'(i,j)|,\\ 0\leqslant i\leqslant m-1,0\leqslant j\leqslant n-1\end{matrix}\right\} \tag{7}$$

差值图像的实际意义是比较两幅二值图像之间的差异，如果相应像素点的像素值相等，则在差值图像上像素值为 0，即表现为白色点；反之则为 1，表现为黑色点。差图像中，某个像素的 8 邻域中没有一个检测错误的点(即黑点)，则称该像素为稀疏点；若其 8 邻域中至少有一个检测错误点，则称之为稠密点。于是可由水印差图中稀疏点与稠密点的比值来判断攻击类别，首先定义如下规则：

ϕ={差图像中像素点总数}；

ϕ_s={差图像中稀疏点的像素点总数}

ϕ_d={差图像中稠密点的像素点总数}

$$\rho=\frac{\phi_s}{\phi},\ \mu=\frac{\phi_s}{\phi_d}$$

攻击类型判断方法如下：

$$\begin{cases}\text{图像未收到攻击}, & \text{if}(\rho=0);\\ \text{可接受的攻击}, & \text{if}(\rho>0\ \text{and}\ \mu<T);\\ \text{恶意攻击}, & \text{if}(\mu\geqslant T)。\end{cases} \tag{8}$$

阈值 T 取值越大，对恶意攻击的判断条件就越严格，算

法安全性也就越高。实验中 T 取值 0.8。

对恶意攻击的篡改定位，我们可以采用文[8]类似的方法，用数学形态学的方法滤除干扰信息以得到一个紧凑的篡改区域。

4 实验结果

本文算法在 Visual C++ 6.0 环境下得到实现。实验中公式(6)中阈值 α 取 0.5，我们以 256×256×24 的彩色图像作为原始载体图像，水印图像以一幅 256×128×2 的二值图像为例，图 2 给出了一个水印嵌入实例。

(1)透明性实验

实验中，我们采用了大量不同载体图像(256×256×24)和水印图像进行透明性实验，部分结果如表 1 所示。

表 1 嵌入不同水印图像的 PSNR(单位：dB)

嵌入容量	Lena	Airplane	Peppers	Splash
1024bit	49.02	60.49	51.23	49.32
4096bit	43.75	55.96	39.67	44.74
32768bit	39.58	38.47	37.33	40.70

a.原图像　b.水印

c.含水印图像　d.提取水印

图 2 水印嵌入实例

当水印嵌入容量控制在 1024bit 以内时，含水印图像的 PSNR 值一般都在 49dB 以上，图像具有较好的视觉效果，说明本文水印算法透明性非常好。

(2)对非恶意攻击的鲁棒性

本文算法对视觉可接受的一般图像处理操作具有一定鲁棒性，表 2 给出了一些常见的非恶意攻击测试结果，实验中采用归一化相关值 NC(normalized cross-correlation)[7]来评价提取水印质量。从表 2 中发现，含水印图像即使遭受到一定的图攻击之后，我们仍然能从中提取水印以证明版权。

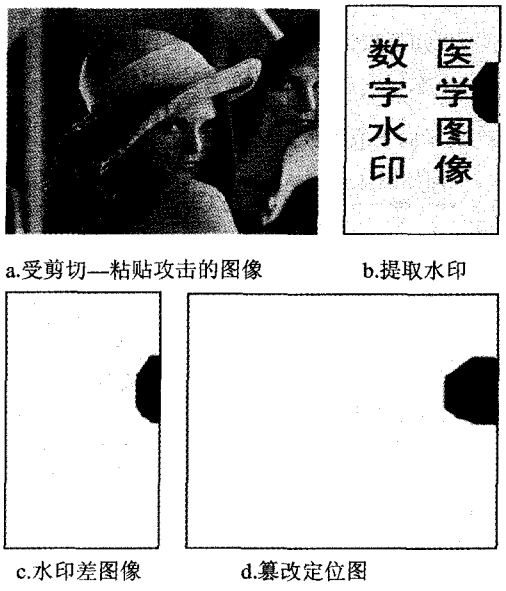
(3) 图像认证

本小节对提出算法的脆弱性和篡改检测与定位能力进行实验，通过对水印差图像进行数学形态滤波以形成一个紧凑的篡改区域，图 3 给出了剪切—粘贴攻击的篡改检测定位实验，白色区域表示非篡改区，黑色区域表示篡改区。

表 2 对非恶意攻击的鲁棒性实验

攻击	质量因子为 40 的 JPEG 压缩	低通滤波	图像边缘锐化	直方图均衡	3% 椒盐噪声	3% 高斯噪声
NC	0.6743	0.9471	0.9596	0.9894	0.9502	0.7258

结论 本文提出了一个医学图像半脆弱水印算法。算法通过自适应地修改整数 Harr 小波变换后高频系数以嵌入水印。算法中采用可逆颜色变换和整数 Harr 小波变换，避免浮点计算引起的精度舍入误差，有助于提高水印算法透明性；同时对高频系数的修改与其大小相自适应，进一步保证了水印透明性。实验结果也证明，该算法在保证较高水印透明性同时，对一般图像攻击具有一定鲁棒性，并且能对恶意攻击进行检测与定位，形成一个紧凑的篡改区域。嵌入水印图像的高透明性确保其能用于医疗诊断，不会干扰医生的医疗诊断，本算法能应用于医学图像的管理与保护实践。



a.受剪切—粘贴攻击的图像　b.提取水印

c.水印差图像　d.篡改定位图

图 3 对恶意攻击的篡改定位

参 考 文 献

1 黄夏菱，刘红梅. 一种无失真数据隐藏算法. 中山大学学报(自然科学版)，2002,41(6):18～21

2 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. 中国图象图形学报，2006,11(5):736～741

3 Goljan M, Fridrich J J, Du R. Distortion-free data embedding for images [C]. In: Proceedings of the 4th International Workshop on Information Hiding, Pittsburgh, PA, USA, 2001

4 Honsinger C W. A Robust Data Hiding Technique Based on Convolution with a Randomized Phase Carrier. In: Proc. of PICS'00, Portland, Oregon, 2000

5 史忠植. 知识发现. 北京:清华大学出版社，2002

6 闫伟齐，邹建成，齐东旭. 一种基于 DES 的数字图像置乱新方法. 北方工业大学学报，2002,14(1): 1～7

7 杨恒伏，陈孝威. 小波域鲁棒自适应公开水印技术. 软件学报，2003, 14(9):1652～1660

8 Bartollini F, Tefas A, Barni M, Pitas I. Image Authentication Techniques for Surveillance Applications. In: Proc. of IEEE, 2001, 89(10):1403～1418