

# 一种适用于远程医疗的水印算法

王 刚, 饶妮妮, 张 瑛

(电子科技大学生命科学与技术学院 成都 610054)

**【摘要】**研究了脑电图(EEG)的水印算法,提出了一种基于自适应滤波的数字水印算法。实验仿真结果表明水印是不可见的,经过低通滤波、中值滤波、维纳滤波、JPEG压缩、小角度旋转等图像处理操作后仍可检验出水印,比空域算法有更高的鲁棒性。

**关键词** 数字水印; 自适应滤波; 远程医疗; 脑电图

中图分类号 Q-33 文献标识码 A

## A Novel Watermarking Algorithm for Telemedicine

WANG Gang, RAO Ni-ni, ZHANG Ying

(School of Life Science and Technology, Univ. of Electron. Sci. & Tech. of China Chengdu 610054)

**Abstract** Modern telecommunication infrastructure supports the possibility of delivering quality health care without the physical presence of medical experts. The integrity of medical signals being transmitted through communication channels must be established before utilization. In this paper, we study the watermarking algorithms for electroencephalogram (EEG) and put forward a novel watermarking algorithm based on adaptive filter. The experimental results show that the watermark is invisible and the watermark algorithm is robust against the most common image manipulations, such as JPEG lossy compression, low-pass filtering, median filtering, Wiener filtering, noise addition and rotation.

**Key words** digital watermark; adaptive filter; telemedicine; electroencephalogram

数字水印是在数字信号内容之中嵌入某种不可感知的信息,这种嵌入的信息对于整体来讲是不可见的,而在用于认证的时候又能够被提取出来。这种嵌入水印的数据不但可以用于远程医疗中的实时诊断,还可以应用于教研活动<sup>[1]</sup>。目前国际上针对远程医疗的水印算法的研究还较少,且大多是针对空域的,这种空域算法对通常的信号处理鲁棒性不好。为了提高医学信号水印算法的鲁棒性,本文对医学信号在小波域的水印算法<sup>[2]</sup>进行了研究。将一类混合混沌序列与水印图像结合,增加系统的抗破译能力,嵌入到医学信号小波分解的低频子带中。

### 1 水印算法的预处理

#### 1.1 脑电信号的压缩与小波变换

在一般的脑电图(ElectroEncephaloGram, EEG)实验室中,采用AR模型压缩EEG信号。本文实验中,实测的EEG采样率是250 Hz,采样电极是30个,得

到了 $30 \times 496$ 的EEG数据。利用AR模型对每个电极测得的数据进行拟合,AR模型的阶数为15,采用Levison-Durbin递推算法,从而把每个电极采得的496个数据压缩为16个系数与480个预测误差。图1、2给出了EEG数据和误差数据。

在远程通信中,预测误差数据是需要传送的,因此要对误差数据嵌入水印,以确保脑电信号的真实性和安全性。把这些数据看作一个二维图像数据,其大小为 $30 \times 480$ 。

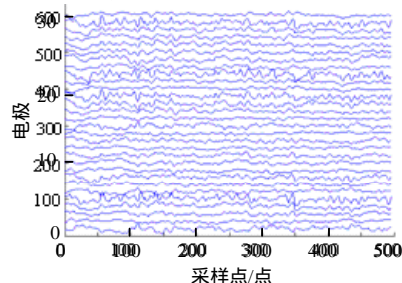


图1  $30 \times 496$ 的EEG数据

收稿日期: 2005-05-23

基金项目: 教育部科学技术研究重点项目(03146)

作者简介: 王 刚(1977-), 男, 博士生, 主要从事图像处理、盲信号处理方面的研究。

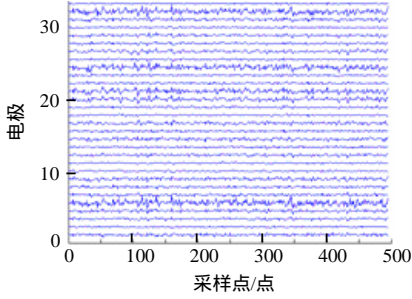


图2 30×480的预测误差

用  $I$  表示尺度为  $M \times N$  的原始图像,  $Y$  表示  $I$  的三级离散小波变换分解。在水印提取的时候, 也要用到相同的小波变换, 所以算法中使用的小波也可作为密钥的一部分。大量理论分析表明, 对于图像来说, 表征它的最主要部分是低频<sup>[3]</sup>, 而高频大部分点的数值均接近 0, 频率越高, 该现象越明显, 所以高频部分不利于水印的嵌入, 本文建议将水印信号嵌入到  $L_{L_3}$  部分, 如图 3 所示。  $L_{L_3}$  称为待嵌入数据, 用  $L_n$  表示。

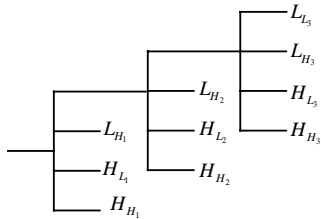


图3 三级小波分解示意图

### 1.2 混合混沌序列与水印序列的产生

将混沌序列引入水印信号可以有效地提高水印信号抗攻击的能力。近年来, 已有混沌序列被应用于水印的产生<sup>[4]</sup>。本文提出将一类新的混合混沌序列引入水印信号。混合混沌序列  $\{m_n\}$  的产生方法如图 4 所示。该序列综合了 Logistic 混沌序列和  $m$  序列的优点, 克服了两者的缺点, 能够克服有限精度效应对混沌序列的影响, 保障混沌序列良好地伪随机性和周期可控性<sup>[5]</sup>。

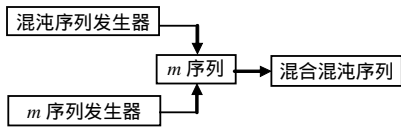


图4 混合混沌序列产生方框图

本文中, 要嵌入的水印信息  $H$  是一组  $M_1 \times M_2$  的二值图像。为了把它与混沌序列进行调制, 必须把它转换成一维数组  $v_n$ , 再把水印信号  $v_n$  与长度为  $M_1 \times M_2$  的混合混沌序列  $m_n$  进行调制, 形成新的水印序列  $S_n$ 。采用异或运算实现调制, 即:

$$S_n = v_n \oplus m_n \quad v_n, m_n \in \{0, 1\} \quad (1)$$

式中  $\oplus$  表示异或运算。

### 1.3 自适应滤波器原理

本文希望已嵌入水印信号的图像经各种攻击的操作后, 仍然能从中提取原始水印信号, 经分析发现, 提取最佳水印信号的过程实质是一种最佳滤波过程, 因此本文提出采用自适应滤波技术来提取嵌入到医学信号中的水印信号。应用横向结构的 FIR 滤波器形式来实现自适应滤波器是最常用的一种方法, 如图 5 所示。这里,  $x_j(x_{1j}, x_{2j}, \dots, x_{Nj})$  是输入向量  $X_n$  的第  $j$  个向量; 其加权系数是一组向量  $w_j(w_{1j}, w_{2j}, \dots, w_{Nj})$ ;  $y_j$  是系统输出向量  $Y_n$  的第  $j$  个标量, 系统输出  $Y_n$  等于  $F_n$  的估计;  $d_j$  是参考输入(或期望输出)  $D_n$  的第  $j$  个标量。通过调整加权系数  $w_n$  使得系统的均方误差最小。

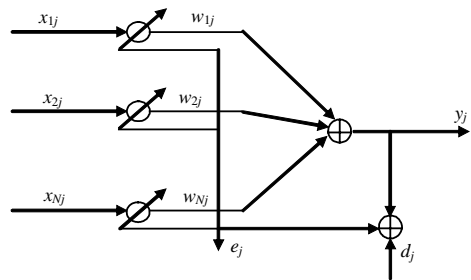


图5 自适应滤波器的原理图

### 1.4 自适应抵消器

自适应抵消器是自适应滤波器的应用。当用作自适应抵消器时, 原始信号为  $X_n = F_n + U_n$ , 参考信号与干扰  $U_n$  有关, 与信号  $F_n$  无关。把原始输入加到自适应滤波器的  $d_j$  端, 参考输入加到  $x_j$  端。自适应滤波器接受误差  $e_j$  的控制调整  $w_j$ , 使得它的输出  $y_j$  趋于等于  $d_j$  中与它相关的  $u_j$ , 于是,  $e_j$  作为  $d_j$  与  $y_j$  之差就接近等于信号  $f_j$  (信号向量  $F_n$  的第  $j$  个元素)。

## 2 水印的嵌入与提取

### 2.1 水印的嵌入

本文的工作要把  $S_n$  嵌入到  $L_n$  中, 采用的嵌入方法为:

$$g_j = l_j + \alpha s_j \quad 0 \leq j < M_1(M_2 - 1) \quad (2)$$

式中  $s_j$  是  $S_n$  (水印序列) 的元素;  $l_j$  是  $L_n$  (原始图像的小波系数) 的元素;  $g_j$  是  $G_n$  的元素,  $G_n$  为嵌入水印后图像的小波系数;  $\alpha$  为嵌入水印的强度(鲁棒因子), 与水印鲁棒性成正比。通过对  $G_n$  进行小波反变换, 就得到了嵌入水印后的图像。

### 2.2 水印的提取

嵌入水印后的图像, 经过各种攻击处理后, 进行小波变换, 在相应的低频子带上:

$$g'_j = g'_j + \alpha s'_j \quad (3)$$

式中  $s'_j$  是  $S'_n$  (检测出的水印序列) 的元素;  $l'_j$  是  $L'_n$  的元素,  $L'_n$  是原始图像小波系数经各种攻击处理后的结果, 其主要成分与原始图像相应的小波系数  $L_n$  相关;  $g'_j$  是  $G'_n$  的元素,  $G'_n$  表示待检验水印图像小波系数中相应嵌入水印信息的部分。按照自适应抵消器的原理, 把参考输入  $L_n$  加到  $x_j$  端,  $G'_n$  加到自适应滤波器的  $d_j$  端, 自适应滤波器接受误差  $e_j$  的控制调整  $w_j$ , 使得它的输出  $y_j$  趋于等于  $G'_n$  中与它相关的  $L'_n$ , 于是  $e_j$  作为  $d_j$  与  $y_j$  之差就接近等于信号  $\alpha \times S'_n$ 。

对得到的信号  $e_j$  进行量化处理成 0、1 序列  $S'_n$ , 再与原始的混合混沌序列  $\{m_n\}$  进行异或, 就可得到估计的原始水印序列为:

$$v'_n = S'_n \oplus m_n \quad (4)$$

最后, 把一维的序列转化为二维的图像, 即为估计的嵌入原始信息。

### 3 数值仿真

#### 3.1 实验条件与检测指标

在  $30 \times 480$  的脑电信号误差数据中, 按照上述算法加入水印, 采用 “haar” 小波对图像进行小波分解。水印图像是写有 “生命学院” 标志的  $14 \times 61$  二值图像。水印的鲁棒性检验采用  $P_{\text{PSNR}}$  (峰值信噪比) 和  $N_{\text{NC}}$  两个指标来检测。由于误差数据比较小, 实验中把它扩大 10 倍。

$$\begin{cases} P_{\text{PSNR}} = 10 \lg \left[ \frac{255^2}{M_{\text{MSE}}} \right] \\ M_{\text{MSE}} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (X_{ij} - X'_{ij})^2 \end{cases} \quad (5)$$

式中  $M$ 、 $N$  分别为图像的长度和宽度;  $X_{ij}$  表示原始图像像素灰度值;  $X'_{ij}$  表示加入水印后的图像像素的灰度值。  $P_{\text{PSNR}}$  值越大, 加入水印后的图像失真越小。

$$N_{\text{NC}} = \frac{\sum W W'}{\sum W^2} \quad (6)$$

式中  $W$  为原始水印;  $W'$  为提取出来的水印。  $N_{\text{NC}}$  值越大, 检测效果越好。

#### 3.2 结果与分析

JPEG 压缩标准是检测水印算法鲁棒性的一个常用标准。表 1 所示为该标准检测的结果。

表1 JPEG压缩实验

| 攻击方法                        | JPG(70)  | JPG(50)  | JPG(30)  |
|-----------------------------|----------|----------|----------|
| $P_{\text{PSNR}}/\text{dB}$ | 27.639 2 | 27.559 8 | 27.466 7 |
| $N_{\text{NC}}$             | 0.951 4  | 0.941 4  | 0.915 7  |

JPEG 压缩对图像影响比较大。在有损压缩条件

下, 本算法仍能提取出有效的水印。对于通常的信号处理, 表 2 所示给出了测试结果。

表2 一般信号处理实验

| 攻击方法                        | Wiener<br>(3×3) | Medfilter<br>(3×3) | Medfilter<br>(5×5) |
|-----------------------------|-----------------|--------------------|--------------------|
| $P_{\text{PSNR}}/\text{dB}$ | 42.581 6        | 36.741 8           | 35.826 7           |
| $N_{\text{NC}}$             | 0.993 9         | 0.931 0            | 0.819 6            |

表 2 中, Wiener(3×3) 表示滤波器的窗口大小为 3×3, 噪声功率是 1; Medfilter(3×3) 表示中值滤波, 模板是 3×3; Medfilter(5×5) 表示中值滤波, 模板是 5×5; Butterworth LP 表示截止频率为 50 的 2 阶 Butterworth 低通滤波器。  $P_{\text{PSNR}}$  值越大, 说明信号处理对原图像造成的失真越小, 这样提取的水印越清晰, 即  $N_{\text{NC}}$  值越大。显然, Wiener(3×3) 和 2 阶 Butterworth 低通滤波器对原图像造成的损失小, 而中值滤波对原图像造成的损失较大。

表 3 所示为噪声攻击下的检测结果。其中 “高斯噪声 1” 和 “高斯噪声 2” 分别代表均值为 0、方差为 2 和均值为 0、方差为 3 的高斯白噪声。实验表明, 随着噪声强度的加强,  $P_{\text{PSNR}}$  值降低, 即图像的失真度加强, 提取的水印质量下降。表 4 所示显示了小角度图像旋转的检测结果。

表3 高斯噪声实验

| 攻击方法                        | 无噪声      | 高斯噪声1    | 高斯噪声2    |
|-----------------------------|----------|----------|----------|
| $P_{\text{PSNR}}/\text{db}$ | 50.156 3 | 46.150 8 | 43.886 8 |
| $N_{\text{NC}}$             | 1        | 0.992 8  | 0.928 6  |

表4 旋转攻击实验

| 攻击方法                        | 旋转0.5/(°) | 旋转0.5/(°) |
|-----------------------------|-----------|-----------|
| $P_{\text{PSNR}}/\text{db}$ | 43.270 2  | 42.780 9  |
| $N_{\text{NC}}$             | 0.931 4   | 0.924 3   |

#### 3.3 讨论

以上四组实验, 不同组选取的  $\alpha$  (表示嵌入水印的强度的鲁棒因子) 不尽相同, 但在同组实验中选取的  $\alpha$  相同。在实际应用中, 可以根据需要采用不同的鲁棒因子。如为了抵抗 JPEG 攻击和小角度旋转攻击, 鲁棒因子必须选得大一些; 为了在传输中抵抗高斯噪声的攻击, 鲁棒因子可以选的小一些, 从而提高图像质量。在应用中, 可以公开算法, 利用混合混沌序列的密钥恢复水印, 从而抵抗稳健性攻击。

(下转第 157 页)

方法,是把定性因素定量化,将人的主观判断用数学表达式进行处理,并能在一定程度上检验和减少主观影响,使评估更趋于科学化<sup>[6]</sup>。

将AHP法运用在城市政府管理评估指标体系中,政府就可对照指标,判断自身是否具备进行特殊性属性的城市建设的必要性和可行性。当然,仅依靠城市政府管理指标体系对一个城市进行定性也是不全面的,政府还要依据其他体系对照分析,如:基础支持体系、科技体系、人口体系、生态体系等。

其实,所谓评估是根据确定的目的来测定对象系统的属性,并将这种属性变为客观定量的计算值或主观效用的过程,是选优和决策的基础。评估一般来讲是复杂并且困难的,往往带有多目标、多指标的特征。对于城市管理评估指标,要求能同时考虑到经济和人文的多方面准则,并能给予定量描述和运算。经济性的客观指标是较为硬性的,是基本的;而人文准则则包括了社会文化、政府行为、公共道德等,偏重于主观、较为软性的,但也是必不可

少的<sup>[7-8]</sup>。

#### 参 考 文 献

- [1] 吴贻永,葛震明. 联合国城市指标体系概述与评价[J]. 城市问题, 2001, (3): 13-15.
- [2] 朱世辉,杨春,李树勇,等. 结合层次分析法的模糊综合评价模型及其应用[J]. 实验科学与技术, 2006, 4(3): 42-44.
- [3] 张新红. 城市可持续发展能力综合评价研究——以成都市为例[D]. 成都: 成都理工大学, 2005.
- [4] 闪媛媛. 休闲城市指标体系研究[D]. 杭州: 浙江大学, 2005.
- [5] 范杰. (高)科技型城市的指标体系内涵及其创新战略重点[J]. 地理科学, 2002, (12): 642-648.
- [6] 翟丽. 质量功能展开技术及其应用综述[J]. 管理工程学报, 2000, (1): 52-65.
- [7] 姜旭. 生态城市建设水平和措施研究[D]. 长春: 吉林大学, 2005.
- [8] 吴志强,蔚芳. 可持续发展——中国人居环境评价体系[M]. 北京: 科学出版社, 2003.

编辑 漆蓉

(上接第142页)

## 4 结 论

本文提出了一种基于自适应滤波的数字水印算法,并有效地应用于远程传输的脑电信号中。仿真结果表明水印是不可见的;经过图像处理操作后具有鲁棒性,而一般的空域算法经过以上信号处理后往往失效。混合混沌序列的引入保证了水印的安全性。因此,该数字水印算法可以进一步推广应用于远程医疗系统的其他医学信号中,用以保护医学信号的完整性。

#### 参 考 文 献

- [1] KONG X. Watermarking medical signal for telemedicine[J].

IEEE Trans Information Technology in Biomedicine, 2001, 5(3): 195-201.

- [2] PODILCHUK C I, ZENG W. Image-adaptive watermarking using visual models[J]. IEEE Journal on Special Areas in Communications, 1998, 16(4): 525-539.
- [3] MALLAT S G. A theory for multiresolution signal decomposition: the wavelet representation[J]. IEEE Trans Pattern Anal. Machine Intell. 1989, 11(7): 674-693.
- [4] YANG J, LEE M H, CHEN X H, et al. Mixing chaotic watermarking for embedding in wavelet transform domain[C]//ISCAS2002, Arizona, USA, 2002: 668-671.
- [5] 饶妮妮. 一类混合混沌序列及其特性分析[J]. 电子科技大学学报, 2001, 2: (30) 115-119.

编辑 孙晓丹