文章编号:1000-582X(2010)06-134-05

小波突变点检测的扩频掩密分析算法

杨艳秋[1],李建勇[2],曹长修[1]
(1.重庆大学 自动化学院,重庆 400044;2.重庆通信学院,重庆 400035)

摘　要:研究了音频信息隐藏技术中的"知彼"问题——掩密分析方法。该算法首先对含密音频进行小波去噪处理,然后进行滑动相关计算,最后利用小波突变点检测技术提取特征对待分析的音频进行分类,该算法检测性能具有只受秘密信息嵌入强度影响而与嵌入容量无关的特点。实验结果表明,含密音频中 PN 序列嵌入强度越大,检测的正确率越高。特别在嵌入强度只有 0.002 时,算法的检测正确率仍然达到了 80%以上,因此,算法具有良好的检测性能。

关键词:音频掩密分析;扩频;去噪; 突变点检测;小波变换
中图分类号: TP391　　**文献标志码**:A

A spread spectrum steganalysis algorithm based on discontinuity detection

YANG Yan-qiu[1], *LI Jian-yong*[2], *CAO Chang-xiu*[1]
(1. College of Automation Chongqing University, Chongqing 400044, P. R. China;
2. Chongqing Communication Institute, Chongqin 400035, P. R. China)

Abstract: A novel audio steganalysis method is proposed.. the audio signal is denoised with wavelet transform. Then, a part of noise signal with different length is intercepted circularly and is used to calculate the cross-correlation sequence with the rest of the noise signal. With the wavelet discontinuity detection technique, the feature is extracted from the cross-correlation sequence for steganalysis and find out the steg-audio. The detection rate is determined by the embedding strength of the secret message other than the embedding capacity. Experimental results show that the more embedding intensity of PN sequence is, the higher the detection rate will be. The detection rate of the algorithm is above 80% when the strength of the PN sequence is about 0.002, which demonstrates that the proposed algorithm has good detection performance.

Key words: audio steganalysis; spread spectrum; denoising; discontinuity detection; DWT

数字掩密分析(steganalysis)技术则是以揭示媒体中秘密信息的存在性为目的的,它与掩密技术是相对立的。掩密与掩密分析技术在国家安全、情报、军事方面具有重要的意义,因此受到了各国政府、情报机关及军事机构的广泛关注和支持研究。

以数字音频为载体的掩密技术近年来发展迅速,已经提出了许多掩密算法。然而,近年来针对音频的掩密分析算法很少。文献[1]提出的算法可以有效检测经过 LSB 方式掩密了的音频,但是不适用于其它掩密算法。Harmsen[2]等人建立了通用的加性噪声掩密分析模型,得出含密媒体的直方图的频率质心下降的结论;但无法有效区分原始音频和含

收稿日期:2010-02-10
基金项目:国家自然科学基金资助项目(No. 6067215);重庆市自然科学基金资助项目(No. CSTC 2007BB2105)
作者简介:杨艳秋(1979-),女,重庆大学博士,主要从事音频信息隐藏及智能控制方向研究,(Tel)13648419925;
(E-mail)yangyangiul@163.com。

密音频。Johnson[3]等人则是利用含密音频和原始音频的语谱图若干特征作为特征矢量，该算法只对LSB 掩密方法和 Hide4PGP 掩密工具掩密的音频进行了实验，检测性能受嵌入容量的制约，并且不能估计嵌入容量。Xue-min Ru[4]等人则提出了一种在小波域利用线性预测技术提取小波系数特征，利用SVM 进行分类的掩密分析算法，在秘密信息嵌入容量较大时，具有较高的检测正确率。Altun[5]等人是根据音频掩密引入的加性高斯白噪声在形态学上引起的失真来检测，但是检测的准确性有待进一步提高。淦新富[6]等人则提出了一种基于主元统计的音频隐写分析方法。该算法分别从时域、小波域、频域提取音频掩密前后不重要的主元，形态学变换后，以其相邻两列汉明距离的奇数阶中心矩作为特征向量，用 SVM 进行分类，具有比较高的检测准确率。

以上分析可以看到，在已有的音频掩密分析算法中，只有文献[6]提出的算法对扩频掩密算法进行了检测实验，但实验中未给出扩频掩密算法的具体嵌入强度等参数，并且不能检测出秘密信息的嵌入容量。针对经典音频扩频掩密算法的特点，提出了一种基于小波突变点检测技术的音频扩频掩密分析算法。实验证明，该算法可以有效区分自然音频和含密音频，同时还可以检测出嵌入的 PN 序列的长度，从而可以确定秘密信息的平均嵌入容量。

1　音频扩频掩密原理

音频扩频掩密技术利用扩频的思想，将待嵌入的秘密信息比特扩展为一定长度的 PN 序列，然后叠加在载体音频信号之上，实现秘密信息的嵌入。由于 1 bit 的秘密信息被扩展为一个 PN 序列并叠加在了音频信号大量的采样点之上，因此具有良好的鲁棒性，使得该技术受到广泛关注，并有大量的算法被相继提出[7-8]，总结这些扩频算法，其嵌入过程如图 1 所示

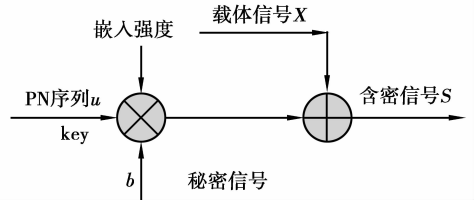


图 1　音频扩频嵌入通用模型

在该模型中，PN 序列由密钥生成，双极性的秘密信息比特用 PN 序列进行扩展后与载体信号相叠加。载体信号可以是时域信号，也可在 DCT、DWT 等变换域上。这里不妨假设 PN 序列与时域信号相叠加。

假设原始信号待嵌入帧的采样点表示为 $\boldsymbol{X}=(x_1,x_2,\cdots,x_L)$，$x_i$ 表示该帧第 i 个采样点，每帧长 L。嵌入的 PN 序列表示为 $\boldsymbol{u}=(u_1,u_2,\cdots,u_L)$。嵌入的比特信息为 b，$b\in\{-1,1\}$，嵌入强度 $\alpha\in(0,1)$，一般取值比较小。则音频扩频秘密信息嵌入通用模型用公式可以表示为

$$\boldsymbol{S}=\boldsymbol{X}+b\alpha\boldsymbol{u}。\tag{1}$$

提取时，利用密钥产生 PN 序列 $\boldsymbol{u}$，首先利用去噪算法，将音频帧信号中的噪声信号分离出来，然后在噪声信号中再进行秘密信息的相关检测，噪声信号表示为 $\boldsymbol{f}=(f_1,f_2,\cdots,f_L)$，相关计算公式为

$$t=\langle\boldsymbol{f},\boldsymbol{u}\rangle=\frac{1}{L}\sum_{i=1}^{L}f_iu_i。\tag{2}$$

而提取的秘密信息比特

$$\tilde{b}=\mathrm{sign}(t)。\tag{3}$$

2　基于小波变换的掩密分析算法

算法中，主要应用小波去噪算法分离音频信号的噪声，应用小波突变点检测技术检测滑动相关计算值中的突变点来提取特征判断音频是否含密。

2.1　小波去噪与突变点检测技术

在扩频掩密模型中，去噪算法可以完成噪声的分离工作。小波去噪的基本思想是：根据噪声与信号在各尺度上的小波谱具有不同表现的特点，将噪声小波谱占主导地位的那些尺度上的噪声小波谱分量去掉，从而达到去噪的目的。采用 D. L. Donoho[9]提出的软阈值小波去噪算法对含密音频进行去噪处理。

小波变换的多分辨率分析思想[10]，可以有效地检测信号的各种突变点，它比经典的 FT 突变点检测方法更有效，并能精确定位突变点的位置。小波突变点监测技术的思想是：对待分析信号进行多级小波分解，并只对小波的第一层高频系数进行信号重构，重构后的信号可以明显地突出突变点及其在信号中的位置。

2.2　相关分析

2.2.1　PN 序列存在性分析

扩频掩密模型中，PN 序列看作是含密音频的噪声。不妨设 PN 序列 u 服从 $N(0,\sigma_u^2)$ 的高斯分布。在秘密信息提取过程中，假设从待提取秘密信息的含密帧上分离出来的噪声信号为 f，则噪声信号应该由原始音频信号本身的噪声 $\boldsymbol{f}'$ 和秘密信息嵌入过程中叠加的 PN 序列 $\boldsymbol{u}$ 组成，即

$$\boldsymbol{f}=\boldsymbol{f}'+b\alpha\boldsymbol{u}。\tag{4}$$

掩密通信的接收方由于知道密钥，又由式(2)，接收端利用 PN 序列与该帧噪声计算得到的相关值 t 的极性，提取该帧嵌入的秘密信息，t 可表示为

$$t=\langle\boldsymbol{f},\boldsymbol{u}\rangle=\langle\boldsymbol{f}'+b\alpha\boldsymbol{u},\boldsymbol{u}\rangle=\langle\boldsymbol{f}',\boldsymbol{u}\rangle+\langle b\alpha\boldsymbol{u},\boldsymbol{u}\rangle=\tilde{f}_1+b\alpha\sigma_u^2。\tag{5}$$

可以看到，知道密钥时，$\tilde{f}_1$ 是提取秘密信息的唯一干扰，它是原始音频信号本身携带的噪声对检测器产生的影响。

信道的监测者可以得到掩密的音频样本，如果他截取一段含密音频，并用去噪算法将该段含密音频上的噪声信号分离出来，这段噪声信号不妨用向量 $\boldsymbol{f}_2$ 表示。假设 $\boldsymbol{f}_2$ 包含一段完整的 PN 序列信息，另外除了 PN 序列信息外，还有其它噪声存在，并且其它噪声所处的位置相对于 PN 序列的位置有多种情况，如图 2 所示

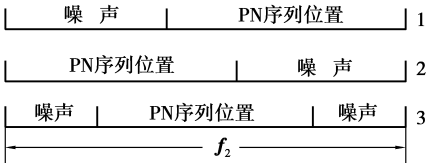


图 2 PN 序列位置与其它噪声相对位置关系

这 3 种位置关系中，为了表述方便，利用第 2 种位置关系表示噪声信号 $\boldsymbol{f}_2$。不妨将其它位置的噪声用向量 h 表示，$\boldsymbol{f}_2$ 用下面的式子来表示：

$$\boldsymbol{f}_2=(\boldsymbol{f}'+b\alpha\boldsymbol{u},\boldsymbol{h})=(f'_1+b\alpha u_1,\cdots,f'_L+b\alpha u_L,h_1,\cdots,h_l)。\tag{6}$$

其中 $f'_i+b\alpha u_i$ 为 PN 序列所在位置处的噪声信号的第 i 个值。

如果监测者使用 $\boldsymbol{f}_2$ 代替 PN 序列，并利用公式(2)、(3)对含密音频进行秘密信息的提取，假设对待提取的含密帧音频进行噪声分离后得到噪声信号 $\boldsymbol{f}_3$，并且二者进行相关计算时 $\boldsymbol{f}_2$ 与 $\boldsymbol{f}_3$ 中的 PN 序列已经相互对齐。为了表述方便，不妨也采用图 2 中的第 2 种位置关系表示 $\boldsymbol{f}_3$，假设 $\boldsymbol{f}_3$ 中其它位置的噪声用向量表示为 $\boldsymbol{K}$，而 PN 序列所在位置处原始音频本身的噪声用向量表示为 $\boldsymbol{f}''$，则

$$\boldsymbol{f}_3=(\boldsymbol{f}''+b'\alpha\boldsymbol{u},\boldsymbol{k})=(f''_1+b'\alpha u_1,\cdots,f''_L+b'\alpha u_L,k_1,\cdots,k_l)。\tag{7}$$

则该含密帧的相关计算的值可表示为

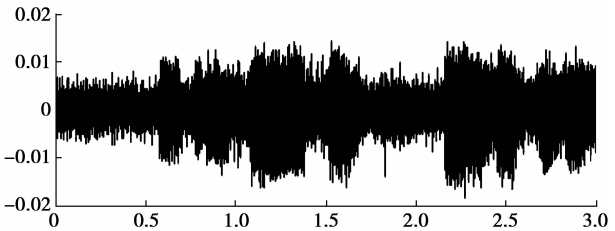
$$\begin{aligned}\tilde{t}&=\langle\boldsymbol{f}_3,\boldsymbol{f}_2\rangle=\langle(\boldsymbol{f}''+b'\alpha\boldsymbol{u},\boldsymbol{k}),(\boldsymbol{f}'+b\alpha\boldsymbol{u},\boldsymbol{h})\rangle=\\&\langle\boldsymbol{f}''+b'\alpha\boldsymbol{u},\boldsymbol{f}'+b\alpha\boldsymbol{u}\rangle+\langle\boldsymbol{k},\boldsymbol{h}\rangle=\\&\langle\boldsymbol{f}'',\boldsymbol{f}'\rangle+\langle\boldsymbol{f}'',b\alpha\boldsymbol{u}\rangle+\langle b'\alpha\boldsymbol{u},\boldsymbol{f}'\rangle+\\&\langle b'\alpha\boldsymbol{u},b\alpha\boldsymbol{u}\rangle+\langle\boldsymbol{k},\boldsymbol{h}\rangle=\\&\hat{f}_1+\hat{f}_2+\hat{f}_3+bb'\alpha^2\sigma_u^2+\hat{f}_4。\end{aligned}\tag{8}$$

由公式(8)也可以看到，在不知道密钥的情况下，仅仅从含密音频中的噪声信号所携带的 PN 序列信息来提取秘密信息时，有 $\hat{f}_1,\hat{f}_2,\hat{f}_3,\hat{f}_4$ 4 项干扰。而知道密钥的情况下，如公式(5)所示，只有 $\tilde{f}_1$ 一项干扰。如果嵌入的 PN 序列强度较大，理论上，$|\alpha^2\sigma_u^2|\gg|\hat{f}_1+\hat{f}_2+\hat{f}_3+\hat{f}_4|$。则可以知道，如果用 $\boldsymbol{f}_2$ 与整个含密音频的噪声信号进行滑动相关计算，则当 PN 序列相互对齐时，所计算的相关值要比不对齐时大的多，因此，可以根据这个特征发现扩频掩密了的音频。

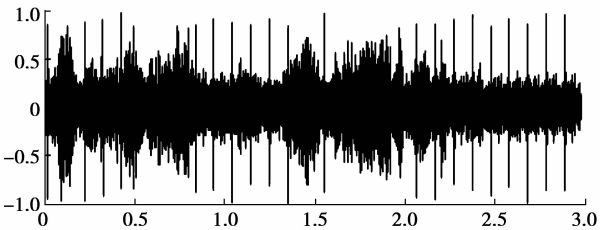
2.2.2 滑动相关值特征分析

在秘密信息相关提取过程中，由于 PN 序列以及含密音频中的噪声信号都服从高斯分布，计算出的相关值也服从高斯分布。如果含有秘密信息，当 PN 序列与噪声信号中的 PN 序列相对齐时，此时相关值的绝对值要远大于其它的相关值的绝对值，因此在此时相关值的一个邻域内，该相关值可以看作是这个邻域内的突变点。

由于秘密信息扩频嵌入过程中，PN 序列是周期性地嵌入到载体音频的，因此，上述的突变点将周期性的出现。可以依此为特征判断音频是否经过了扩频掩秘。图 3 显示了突变点的周期性，在图 3 中，PN 序列强度为 0.005，长度 1 024，服从(0,1)正态分布。由图 3(b)可以看到，突变点具有明显的周期性。



(a)含密噪声信号的滑动相关值序列 ×10⁴



(b)检测后的含密噪声信号的滑动相关值序列 ×10⁴

图 3 小波突变点检测效果及其周期性

3　音频扩频掩密分析算法

以 wav 文件进行掩密分析，首先给出算法的流程图如图 4 所示。结合流程图，给出算法步骤为

Step1：去噪。利用小波去噪算法，对待分析音频 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_{L_1})$ 提取分离出来的噪声信号 $\boldsymbol{f}$ 作为分析对象。

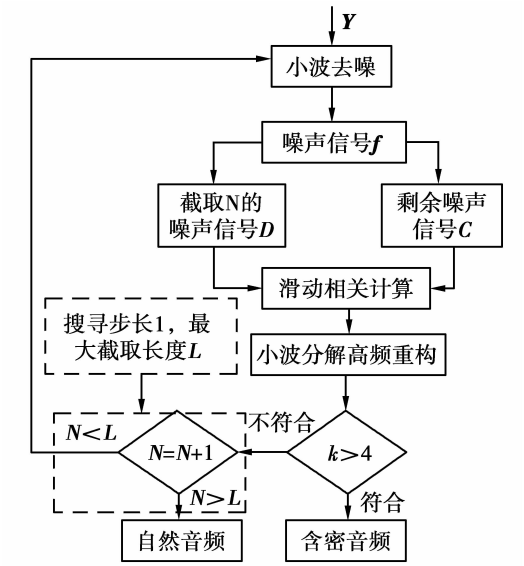


图 4　音频扩频掩密分析流程图

Step2：滑动相关分析。从 $\boldsymbol{f}$ 中连续地截取初始长度为 N_0 的一段噪声 D，与剩余的噪声 C 进行滑动相关计算，得到的第 $i+1$ 个相关值为

$$r_{i+1}=\frac{1}{N_0}\sum_{j=1}^{N_0}d_j c_{(j+i)}。\tag{9}$$

其中 $0\leqslant i\leqslant L_1-N_0-1$，$L_1\gg N_0$，则滑动相关值向量 $\boldsymbol{R}=(r_1,r_2,\cdots,r_{L_1-N_0})$。

Step3：小波分解高频重构。对相关值向量 R 进行六层小波分解，利用第一层高频系数对信号进行重构，重构后的信号表示为 $\boldsymbol{T}=(t_1,t_2,\cdots,t_{L_1-N_0})$。对 $\boldsymbol{T}$ 进行归一化处理。

Step4：对 $\boldsymbol{T}$ 提取特征，其过程为

1）设定阈值 $a=0.5$[16]，当 $\boldsymbol{T}$ 中的值大于 a 时，记录该值在该向量中的位置信息。$\boldsymbol{T}$ 中所有符合条件的位置信息组成一维矩阵 $\boldsymbol{P}$。其中 $\boldsymbol{P}$ 中第 j 个值可表示为：$P_j=i,if|t_i|\geqslant a$。将 $\boldsymbol{P}$ 内的值从大到小排序，得到最终的位置特征矩阵 $\boldsymbol{P}=[P_1,P_2,\cdots,P_k](1\leqslant j\leqslant k)$。

2）如果 $k>4$，对矩阵 $\boldsymbol{P}$ 进行连续的 2 次差分，第一次差分后的矩阵为 $\boldsymbol{E}$，第二次差分后的矩阵为 $\boldsymbol{W}$。再统计 $\boldsymbol{W}$ 中含有 0 的个数 p_1；$\boldsymbol{W}$ 中是否有连续的 3 个或 3 个以上的 0 存在，若存在，$p_2=1$，不妨设 $W_{i-1}=W_i=W_{i+1}=0$，则令 $N_2=E_i$，其中 $2\leqslant i\leqslant k-3$；若不存在，$p_2=0$。如果 $k\leqslant 4$，继续增加截取的噪声 D 的长度，设定最大搜索长度为 L，如果 $N=N+l>L$，循环停止，判定该音频不含有秘密信息。

Step5：含密的判决条件。如果该音频含密，必须满足以下条件

$$p_1>4\&p_2==1\&N_2\geqslant 15。\tag{10}$$

Step6：如果不满足(10)，则令 $N=N+l$，增加截取的噪声 D 的长度，其中 l 为搜索步长。重复 Step1 至 Step5，设定最大搜索长度为 L，如果 $N=N+l>L$，循环停止，判定该音频不含有秘密信息。

4　实验结果及分析

截取 100 个采样率 22.05 kHz，16 bit 量化，长度 16 s 的音频，包括音乐、歌曲等。利用这 100 个音频作为测试样本对所提的掩密分析算法进行测试。先分析 100 个音频样本。再对音频样本进行扩频掩密，得到含密的音频库。秘密信息嵌入时，PN 序列是服从(0，1)正态分布的高斯白噪声，PN 序列嵌入强度从 0.001 到 0.005 不等，PN 序列的长度(即嵌入容量)从 128 到 2 000 不等。利用算法和文献[6]所提算法试验，测试结果为如表 1。

表 1　算法对自然音频以及含密音频测试结果

嵌入强度	算法正确率/%	文献[6] 确率/%
自然音频	100	100
0.001	68.85	45.98
0.002	81.25	66.45
0.003	86.10	76.89
0.004	91.05	89.56
0.005	92.25	90.58

另外，如果判断了某含密音频含有秘密信息，算法能同时给出含密音频嵌入的 PN 序列的长度，实验结果表明，算法给出的 PN 序列长度与含密音频实际嵌入的 PN 序列长度完全符合。

由表 1 实验结果看，对于含密音频的检测，含密音频中 PN 序列嵌入强度越大，检测的正确率越高。特别在嵌入强度只有 0.002 时，算法的检测正确率仍然达到了 80%以上，因此，算法具有良好的检测性能。

5　结　论

讨论并分析了扩频掩密的音频特点，根据这些特点，提出了一种基于小波去噪和突变点检测技术

的扩频音频掩密分析算法。实验表明,该算法具有如下优点:算法的性能不受秘密信息嵌入容量影响,只要秘密信息被连续地嵌入到音频,并且具有一定的嵌入强度,本算法就能检测出来;而且在检测出含密音频的同时,还能确定嵌入的 PN 序列的长度。实验结果表明了该算法具有良好的检测性能。另外,虽然算法主要是针对音频信号进行讨论的,算法同样适用于检测经扩频掩密的其他数据。

算法的不足之处在于只能检测扩频类掩密算法,能够检测多种掩密算法的通用掩密分析算法将是下一步研究的重点。

参考文献:

[1] 李春,黄继武.一种抗 JPEG 压缩的半脆弱图像水印算法[J].软件学报,2006,17(2):315-324.
LI CHUN, HUANG JI-WU. Semi-fragile image watermarking resisting to JPEG [J]. Journal of Software,2006,17(2):315-324.

[2] 王秋生,孙圣和,郑为民.数字音频信号的脆弱水印嵌入算法[J].计算机学报,2002, 25(5):520-525.
WANG QIU-SHENG, SUN SHENG-HE, ZHENG WEI-MIN. The fragile watermark embedding algorithm for digital audio signal[J]. Journal of Computer, 2002, 25(5):520-525.

[3] 吴志军,钮心忻,杨义先.语音隐藏的研究及实现[J].通信学报,2002,23(8): 99-104.
WU ZHI-JUN, NIU XIN-YI, YANG YI-XIAN. Research and implementation for speech information hiding[J]. Journal of Communications, 2002,23(8): 99-104.

[4] FRIDRICH J, GOLJAN M. Detecting LSB steganography in color and grayscale images[J]. IEEE Multimedia and Security,2001, 8(4): 22-28.

[5] HARMSEN J J, PEARLMAN W A. Steganalysis of additive noise modelable information hiding [D]. America: Rensselaer Polytechnic Institute, 2003.

[6] JOHNSON M K, LYU S, FARID H. Steganalysis of recorded speech[C]// Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents VII, January 17-20, 2005, San Jose, CA, USA. [S. l]: IEEE, 2005:664-672.

[7] RU X M, ZHANG H J, HUANG X. Steganalysis of audio: attacking the steghide[C]// Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, August 18-21, 2005, Guangzhou, China. Guangzhou: [s. n.], 2005:3937-3942.

[8] ALTUN O, SHARMA G, CELIK M, et al. Morphological steganalysis of audio signals and the principle of diminishing Marginal Distortions [C]// IEEE International Conference on Acoustics, Speech, and Signal Processing, March 18-23, 2005, Philadelphia, USA. [S. l]: IEEE, 2005:21-24.

[9] 由守杰,柏森,曹巍巍,等. 一种抗 DA/AD 转换的音频信息隐藏算法[J]. 计算机工程与应用, 2008, 44(7): 113-116.
YOU SHOU-JIE, BO SEN, CAO WEI-WEI, et al. Audio information hiding algorithm resisting DA/AD conversions [J]. Computer Engineering and Applications, 2008, 44(7):113-116.

[10] 淦新富, 郭立. 基于主元统计的音频隐写分析[J]. 信息安全与通信保密, 2007(2):63-64.
GAN XIN-FU, GUO LI. Audio steganalysis based on principal component statistics[J]. China Information Security, 2007(2):63-64.

[11] TAVAKOLI E, VAHDAT B V, SHAMSOLLAHI M B, et al. Audio watermarking for covert communication through telephone system[C]// IEEE International Symposium on Signal Processing and Information Technology, August 27-30, 2006, Listel Vancouver Hotel, Vancouver, BC, Canada. Vancouver: IEEE, 2006: 955-959.

[12] GARCIA J, NAKANO M, PEREZ H. Real-Time MCLT audio watermarking and comparison of several whitening methods in receptor side[C]// Proceedings of the Eighth IEEE International Symposium on Multimedia, December 2006 3-5, San Diego, CA, USA. San Diego: IEEE, 2006:991-997.

[13] DONOHO D L. De-noising by Soft-thresholding[J]. IEEE Transactions on Information Theory, 1995, 41(3): 613-627.

[14] 陈伟根,邓帮飞. 小波包能谱熵与神经网络在断路器故障诊断中的应用[J]. 重庆大学学报, 2008, 31(7): 744-748.
CHEN WEI-GEN, DENG BANG-FEI. Applying wavelet packet energy entropy and neural networks to diagnose circuit breaker faults [J]. Journal of Chongqing University, 2008, 31(7):744-748.

[15] 牛奔,李丽.基于 MCPSO 算法的 BP 神经网络训练[J].深圳大学学报, 2009, 26(2): 147-150.
NIU BEN, LI LI. Artificial neural networks training based on MCPSO algorithm[J]. Journal of Shenzhen University, 2009, 26(2): 147-150.

[16] 付忠良. 图象阈值选取方法的构造[J]. 中国图象图形学报, 2000,28(6):36-39.
FU ZHONG-LIANG. Selection of image thresholdon the basis of genetic algorithms[J]. Chinese Journal of Image and Graphics,2000,28(6):36-39.

(编辑 侯 湘)