基于小波变换的语音信息隐藏新方法

吴秋玲*①② 吴 蒙①
①(南京邮电大学通信与信息工程学院 南京 210003)
②(南京理工大学紫金学院 南京 210046)

摘 要：针对音频载体在隐藏机密信息时，存在隐藏容量小、隐蔽性不高和鲁棒性较差等不足，该文提出一种基于小波变换的音频信息隐藏新算法。该算法利用人耳听觉系统对语音信号的中高频信息微小变化不敏感的特性，调节语音段小波变换的中高频系数，进而改变每级小波变换高频系数前后两部分的能量状态来隐藏二进制机密信息。首先测试隐藏深度、隐藏频段和载体语音分段长度 3 个参数对载体语音质量和机密信息误码率的影响，选择算法所需的最佳参数，然后测试算法的可行性和各项评价指标，最后对算法进行常见的 5 种攻击测试。测试结果表明该算法能够实现机密信息的盲提取；具有良好的隐蔽性和鲁棒性，能够抵御加噪、低通滤波、重采样、重量化和回声干扰等多种攻击；具有较大的隐藏容量，且语音分段长度越短，隐藏容量越大。

关键词：信息隐藏；小波变换；高频系数；能量状态
中图分类号： TP391; TP309 **文献标识码**： A **文章编号**：1009-5896(2016)04-0834-07
DOI: 10.11999/JEIT150856

Novel Audio Information Hiding Algorithm Based on Wavelet Transform

WU Qiuling①② WU Meng①
①(*College of Telecommunications and Information Engineering*, *Nanjing University of Posts & Telecommunications*, *Nanjing* 210003, *China*)
②(*College of Zijin*, *Nanjing University of Science and Technology*, *Nanjing* 210046, *China*)

Abstract: In view of the small hiding capacity, low concealment and poor robustness of the audio carrier, a novel audio information hiding algorithm is proposed based on wavelet transform. The algorithm regulates the high-frequency wavelet coefficients in every audio segment, and then changes the energy values of the former and the latter part in each audio to hide confidential information according to the characteristic that human auditory system is not sensitive to small changes in high frequency information of audio. First, the influence of embedded depth, hidden frequency-band and segment length of carrier audio on voice quality and bit error rate is tested to choose the best parameters, then algorithm is verified for the feasibility and robustness by several kinds of common attacking means. Experimental rdsults show that the proposed algorithm, which does not require the original audio signal in the watermark extraction, not only has good concealment and large hiding capacity, but also has strong robustness for resisting the common attacking behaviors, such as noise, low-pass filter, re-sampling, re-quantitative and echo interference. In additional, the audio segment is shorter, the hiding capacity is larger.

Key words: Information hiding; Wavelet transform; High-frequency coefficients; Energy values

1 引言

信息隐藏技术是指将特定的信息嵌入到数字化的载体信息中，在隐藏信息内容的同时也隐蔽信息传播这一行为，以保证密文不引起监控者的注意从而减少被攻击的可能性[1]，其核心技术是信息隐藏与提取算法。与加密技术相比，信息隐藏技术是隐藏信息的存在性，让攻击者无法发现，因此信息隐藏更为安全[2,3]。信息隐藏技术常以语音、文字或图像等媒体类型作为宿主载体。由于图像媒体具有较大的冗余空间，人们常使用图像作为隐藏机密信息的载体，如文献[4]提出一种基于分块自适应压缩感知的可逆水印算法，文献[5]提出一种鲁棒可分离的密文域水印算法。语音是人们最常使用的信息传输方式，是通信系统和互联网传输中最主要的业务类型，因此研究基于语音的信息隐藏技术在保密通信、军

收稿日期：2015-07-16；改回日期：2015-12-11；网络出版：2016-02-19
*通信作者：吴秋玲 redpond2000@163.com
基金项目：江苏省普通高校研究生科研创新计划项目(KYLX_0815)，江苏省高校自然科学研究重点资助项目(10KJA510035)
Foundation Items: Jiangsu Province Postgraduate Scientific Research and Innovation Project (KYLX_0815), Jiangsu Province University Science Research Foundation (10KJA510035)

事情报、版权标记和隐私保护等多个领域具有重要的研究意义和应用价值[6,7]。但是由于语音信号冗余信息较少，且语音传输信道较为复杂，因此国内外针对以语音信号为载体的信息隐藏方法研究还较少[8]。

随着移动通信系统和互联网语音通信的快速发展，近年来更多的国内外专家专注于语音信息隐藏方法的研究，出现了较多的理论和文献。文献[9]提出了一种基于振幅值修改的音频隐写算法，隐蔽性较好。文献[10]提出了一种基于多小波域的水印算法。文献[11]利用人耳对音频的采样倒置不敏感的特性，通过倒置小波系数正负极性隐藏机密信息。文献[12,13]提出基于离散余弦变换的语音信息隐藏方法。文献[14]提出基于奇异值分解的音频信息隐藏方法取得了较好的隐藏效果。通过对当前国内外音频信息隐藏方法分析发现，音频信息隐藏方法主要有空间域隐藏和变换域隐藏两大类[15]，其中变换域方法由于具有很好的透明性和鲁棒性获得了更多的应用[16]，但目前大多数变换域方法还存在一些不足，如算法复杂度高或仅在隐藏容量、隐蔽性和鲁棒性 3 项指标间获得某一项指标的突破，当 3 项指标要求发生变化时往往无法通过调整算法参数来兼顾三者平衡。

本文提出一种基于小波变换的语音信息隐藏的新方法，该方法首先对载体语音进行低通滤波，然后进行多级小波变换，利用人耳对中高频信息微小变化的不敏感，通过比较各级小波高频系数的能量来隐藏机密信息。首先测试在不同隐藏深度、不同隐藏频段和载体语音不同分段长度的情况下载体语音质量和机密信息误码率，选择算法所需的合适参数，然后测试算法的可行性和各项评价指标，最后对算法进行常见的 5 种攻击测试。实验结果显示该方法简单易行，可实现盲检测，具有较大的隐藏容量、良好的隐蔽性和较强的鲁棒性，能够抵御加噪、低通滤波、重采样、重量化和回声干扰等多种攻击。此外，在实际应用中可调整算法参数平衡隐藏容量、隐蔽性和鲁棒性 3 项指标要求。

2　信息隐藏与提取算法原理及参数选择

2.1 信息隐藏原理

人耳所能捕获到的语音信号频率主要分布在 300~3400 Hz 的频段范围内，低于 300 Hz 的低频信号和超出 3400 Hz 以上的高频信号人耳往往难以捕捉。利用人耳听觉系统对语音中高频能量的微小变化不敏感这一特点可以将机密信息隐藏到载体音频信号中。把语音信号按一定时长分段后，对每一段语音进行 r 级小波分解得到高频段、中高频段、中低频段和低频段等多个小波系数。把每一频段的小波系数分为前后两部分，按式(1)和式(2)计算前后两部分的能量，根据机密信息的二进制值按式(3)、式(4)和式(5)调整各级小波系数，得到嵌入机密信息后的系数。

语音段高频系数前半部分能量：

$$\mathrm{EQ}_k=\sum_{s=0}^{N/2^{k+1}}H_k^2(s),\quad k=1,2,\cdots,r \tag{1}$$

语音段高频系数后半部分能量：

$$\mathrm{EH}_k=\sum_{s=N/2^{k+1}+1}^{N/2^k}H_k^2(s),\quad k=1,2,\cdots,r \tag{2}$$

则嵌入机密信息后高频系数为

$$H_k'(s)=\begin{cases}\lambda_{1k}H_k(s), & 0<s<N/2^{k+1}\\ \lambda_{2k}H_k(s), & N/2^{k+1}+1<s<N/2^k\end{cases},\quad k=1,2,\cdots,r \tag{3}$$

$$\lambda_{1k}=\begin{cases}\sqrt{\lambda_k\mathrm{EH}_k/\mathrm{EQ}_k}, & x(k)=1\\ 1, & x(k)=0\end{cases},\quad k=1,2,\cdots,r \tag{4}$$

$$\lambda_{2k}=\begin{cases}\sqrt{\lambda_k\mathrm{EQ}_k/\mathrm{EH}_k}, & x(k)=0\\ 1, & x(k)=1\end{cases},\quad k=1,2,\cdots,r \tag{5}$$

其中，r 为小波分解级数，N 为语音段样点数；$H_k(s)$ 为第 k 级小波分解的高频系数，$x(k)$ 为待嵌入第 k 级高频系数的二进制机密信息；λ_k 为第 k 级高频系数的信息嵌入深度，λ_{1k} 为第 k 级高频系数的前半段放大增益，λ_{2k} 为第 k 级高频系数的后半段放大增益。根据 $H_k'(s)$ 和低频系数 Lr 进行小波逆变换，构建携密语音信号。依据以上设计原理，每一语音段进行 r 级小波分解后可得到 r 组高频系数，则最多可嵌入 r 比特机密信息，但是为了保证信息隐藏算法的隐蔽性和鲁棒性，还需对信息隐藏的频段、嵌入深度和载体语音分段长度等参数进行实验测试，寻找合适参数，在保证算法隐蔽性和鲁棒性的条件下尽量提高算法的隐藏容量。

2.2 信息提取原理

提取机密信息时，首先对携密语音按相同的时长进行分段，然后对每一语音段进行 r 级小波分解，按式(1)和式(2)计算各段语音每一级高频段系数 $H_k'(s)$ 前后两部分的能量 EQ_k' 和 EH_k' ($k=1,2,\cdots,r$)。最后按式(6)提取各级小波高频系数中嵌入的二进制机密信息。

$$x'(k)=\begin{cases}1, & \mathrm{EQ}_k^{'}>\mathrm{EH}_k^{'}\\ 0, & \mathrm{EQ}_k^{'}<\mathrm{EH}_k^{'}\end{cases},\quad k=1,2,\cdots,r \tag{6}$$

2.3 能量变化对语音质量的影响

按2.1节和2.2节所述方法修改语音段前后两部分的能量后，语音段高频系数前后两部分能量$\mathrm{EQ}_k^{'}$和$\mathrm{EH}_k^{'}$，可表述为

$$\begin{aligned}\mathrm{EQ}_k^{'}&=\sum_{s=0}^{N/2^{k+1}}\left(H_k^{'}(s)\right)^2\\&=\begin{cases}\lambda_k\mathrm{EH}_k, & x(k)=1\\ \mathrm{EQ}_k, & x(k)=0\end{cases},\quad k=1,2,\cdots,r\end{aligned} \tag{7}$$

$$\begin{aligned}\mathrm{EH}_k^{'}&=\sum_{s=N/2^{k+1}+1}^{N/2^{k}}\left(H_k^{'}(s)\right)^2\\&=\begin{cases}\mathrm{EH}_k, & x(k)=1\\ \lambda_k\mathrm{EQ}_k, & x(k)=0\end{cases},\quad k=1,2,\cdots,r\end{aligned} \tag{8}$$

语音段前半部分能量变化为

$$\Delta\mathrm{EQ}=\mathrm{EQ}_k^{'}-\mathrm{EQ}_k=\begin{cases}\lambda_k\mathrm{EH}_k-\mathrm{EQ}_k, & x(k)=1\\ 0, & x(k)=0\end{cases} \tag{9}$$

语音段后半部分能量变化为

$$\Delta\mathrm{EH}=\mathrm{EH}_k^{'}-\mathrm{EH}_k=\begin{cases}0, & x(k)=1\\ \lambda_k\mathrm{EQ}_k-\mathrm{EH}_k, & x(k)=0\end{cases} \tag{10}$$

由式(9)和式(10)可见，当嵌入信息为$x(k)=1$时，语音段前半部分能量变化为$\lambda_k\mathrm{EH}_k-\mathrm{EQ}_k$，语音段后半部分能量无变化。当嵌入信息为$x(k)=0$时，语音段前半部分能量无变化，语音段后半部分能量变化为$\lambda_k\mathrm{EQ}_k-\mathrm{EH}_k$。由于语音段前后两部分能量值相差不大，即$\mathrm{EQ}_k\approx\mathrm{EH}_k$，因此嵌入深度$\lambda_k$的选择会影响语音段中一半的高频系数值。由能量计算式(1)和式(2)可知，能量EQ_k是由$N/2^{k+1}$个高频系数进行平方后求和得到的，当EQ_k发生较小变化时，单个高频系数值$H_k(s)$的变化更小，对语音听觉质量影响有限。

2.4 参数选择

为了客观评价隐藏算法的性能，采用语音信噪比SNR(Signal-to-Noise Ratio)、提取的机密信息误码率BER(Bit Error Rate)和PESQ(Perceptual Evaluation of Speech Quality)来评价算法性能。PESQ是ITU-T P.862建议书提供的客观MOS值评价方法，其值在−1～4.5之间，当PESQ>3.5时语音质量较好，达到长途通话质量标准。

$$\mathrm{SNR}=10\lg\left\{\sum_{i=1}^{M}c_i^2\Big/\sum_{i=1}^{M}\left(c_i^{'}-c_i\right)^2\right\} \tag{11}$$

$$\mathrm{BER}=(l/L)\cdot 100\% \tag{12}$$

其中，c_i为原始载体语音，$c_i^{'}$为携密载体语音。L为机密信息总比特数，l为提取的机密信息错误比特数。

2.4.1 信息隐藏频段选择 语音信号经过r级小波分解后产生各个频段下的小波系数，修改任一级小波系数对语音质量都会产生不同程度的影响。

图1所示为经过3级小波(小波库为db1)分解后，4个小波系数在不同嵌入深度λ_k下分别嵌入信息后载体语音SNR曲线对比图(语音分段长度为20 ms)。图2所示为在不同嵌入深度λ_k下，从4个小波系数上提取的机密信息的误码率曲线对比图(40 dB噪声攻击)。图1和图2显示，小波系数的频段越高，载体语音质量下降越少，机密信息隐蔽性越好，但提取的机密信息误码率也越大；频段很低的系数嵌入机密信息后载体语音质量受损严重，但其系数上提取的机密信息误码率几乎为零。可见，载体语音质量和机密信息提取误码率是一对矛盾，在最高频和最低频系数上隐藏信息都是不合适的，可选择在中高频和中低频两个系数上嵌入机密信息。

2.4.2 载体语音分段长度的选择

把载体语音分为10 ms, 20 ms, 30 ms 3种不同长度的语音段，按2.1节所述方法在第2级高频系数上嵌入机密信息，测试语音分段长度对携密载体语音质量和机密信息误码率的影响。

图3为不同语音分段长度下载体语音SNR对比图。图4为不同语音分段长度下提取的机密信息BER对比图(由于在40 dB以上的噪声攻击下算法的误码率为零，因此图4结果是在30 dB噪声攻击下完成的)。图3和图4显示，语音分段长度越短，携密载体语音质量受损越小，提取机密信息的误码率越高。究其原因是因为语音分段长度越短，语音段前后两部分能量越小，按式(3)修改的高频系数变化越小，从而语音质量变化越小，但在白噪声攻击下提取机密信息的误码率越高。此外，语音分段长度越短，单位时间内嵌入的机密信息比特数越多，隐藏容量越大。

2.4.3 嵌入深度λ的选择 图1和图3显示，在嵌入深度λ_k值为1时载体语音的信噪比最高，随着λ_k的逐渐增大，SNR值变小，载体语音质量变差。图2和图4显示，随着λ_k的逐渐增大，提取的机密信息误码率变小。

以上实验结果表明，载体语音SNR、机密信息BER和算法隐藏容量是一组矛盾，在实际应用中，应根据具体指标要求选择合适的信息隐藏频段、嵌入深度和语音分段长度。

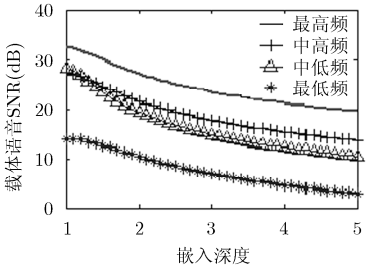

图 1 不同小波系数嵌入信息后语音SNR对比图

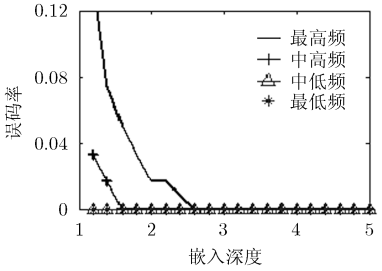

图 2 不同小波系数嵌入信息后机密信息BER对比图

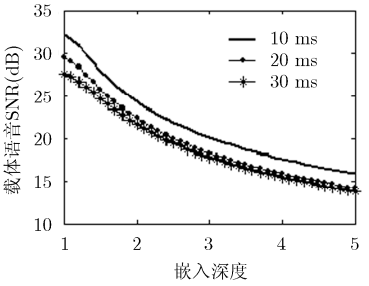

图 3 不同语音分段长度下载体语音 SNR 对比图

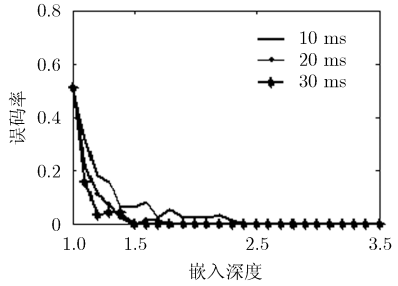

图 4 不同语音分段长度下 BER 对比图

3　基于小波变换的信息隐藏算法的实现

由 2.4 节参数选择可见，选择不同的信息隐藏频段、载体语音分段长度和嵌入深度对携密语音的语音质量、提取的机密信息的误码率以及算法隐藏容量都有不同程度的影响。根据 2.4 节的实验结果，选择以下参数测试算法的各项性能：(1)在经过 3 级小波变换的中高频和中低频系数上隐藏机密信息；(2)中高频系数的隐藏深度 $\lambda_2 = 2$，中低频系数的隐藏深度 $\lambda_3 = 1.5$；(3)语音分段长度为 20 ms; (4)载体语音：采样频率 16 kHz，量化位数 16 bit; (5)机密语音：采样频率 8 kHz，量化精度 8 bit。

3.1 信息隐藏算法步骤

(1)机密信息经过加密和编码形成长度为 L 的二进制比特流 $X = \{x(i), 0 < i < L, x(i) \subset (0,1)\}$，将 X 分为奇偶两组，每组二进制串前各添加 2 组 8 bit 全 1 的信息嵌入开始标记，二进制串后各添加 2 组 8 bit 全 0 的信息嵌入结束标记；

(2)载体语音经过低通滤波(通带截止频率 7 kHz，阻带截止频率 7.8 kHz，通带衰减 3 dB，阻带衰减 40 dB)后被分为 20 ms 长度的语音段 $C = \{c(j), 0 < j < M\}$，M 为语音段数，每一语音段样点数为 N;

(3)对语音段进行 3 级小波分解，得到各级分解的高频段系数 H_1, H_2, H_3 和低频段系数 L_3;

(4)按式(1)和式(2)计算语音段的 H_2 前后两部分的能量 EQ_2 和 EH_2, H_3 前后两部分的能量 EQ_3 和 EH_3;

(5)按给定嵌入深度 λ_2 和 λ_3，根据式(3)、式(4)式(5)将奇数组机密信息嵌入到 H_2 系数中，偶数组机密信息嵌入到 H_3 系数中，获取嵌入后的高频系数 H_2' 和 H_3'；

(6)根据嵌入信息后的各级系数进行小波逆变换，重构载体语音 C'。

3.2 信息提取算法步骤

(1)对携密语音 C' 进行低通滤波后滤除传输过程中产生的带外噪声；

(2)把携密语音 C' 分为 20 ms 长度的语音段 $C' = \{c'(j), 0 < j < M\}$；

(3)对语音段进行 3 级小波分解，得到各级分解的高频段系数 H_1', H_2', H_3' 和低频段系数 L_3'；

(4)按式(1)和式(2)计算各段语音 H_2' 和 H_3' 前后两部分的能量 EQ_2', EH_2', EQ_3' 和 EH_3'；

(5)按式(6)提取每段语音中的二进制信息。当出现 2 组 8 bit 全 1 的信息提取开始标记后，开始提取机密信息直到出现 2 组 8 bit 全 0 的提取结束标记时结束。每一语音段可提取 2 bit 信息。16 bit 的开始或结束标记中出现 2 bit 以下误码时可忽略不计；

(6)将所有语音段提取的已加密机密信息重新组合并解密后恢复出机密信息。

4　实验测试及结果分析

在无攻击情况下按 3.1 节和 3.2 节所述步骤进行实验测试。机密信息为一段时长 674 ms 的语音“南京”，载体语音为录制的涵盖中文男声、中文女声、英文男声和英文女声共 4 种类型的 20 条语音。

4.1 算法隐蔽性与隐藏容量分析

在 20 条载体语音上隐藏机密信息，每条语音做 10 次测试，总共进行 200 次测试。实验所得结果取均值列于表 1 中。其中 SNR_1 为载体语音的信噪比、$PESQ_1$ 为载体语音客观评分值，SNR_2 为提取的机密语音信噪比，$PESQ_2$ 为载体语音客观评分值，BER 为提取的机密语音误码率，Cap 为算法隐藏容量。由于算法在每个长度为 20 ms 的语音段上隐藏 2 bit 机密信息，因此隐藏容量 Cap=2/20(bit/ms)=100 bit/s。表 1 结果显示，载体语音具有较高的信噪比，且 PESQ 值在 3.8 以上，人耳基本感觉不到载体语音的细微变化，因此算法具有良好的隐蔽性和较高的隐藏容量。此外，不同语种的载体语音对语音质量和误码率略有影响。

4.2 算法可行性测试与分析

图 5 为某段载体语音嵌入机密信息前后的波形对比图(截取部分波形)，由图 5 以及表 1 中载体语音的 SNR_1 和 $PESQ_1$ 实验数据可见，载体语音波形图和语音质量未发生明显变化，说明算法具有较好的隐蔽性。图 6 为机密信息提取前后的波形对比图，由图 6 及表 1 中机密信息的 SNR_2, $PESQ_2$ 和 BER 实验数据可见，机密信息波形未发生明显变化，且提取的 BER 值非常小，即算法能够在保证载体语音质量的条件下隐藏机密信息。

4.3 算法鲁棒性测试与分析

信息隐藏算法的鲁棒性是评价算法性能的重要指标，把原始载体语音和携密载体语音同步进行以下常见的 5 种攻击测试，从被攻击后的原始语音信噪比 SNR、携密语音信噪比 SNR_1、机密语音信噪比 SNR_2、原始语音质量 PESQ、携密语音质量 $PESQ_1$、机密语音质量 $PESQ_2$ 以及提取的机密信息误码率 BER 等指标评价算法的鲁棒性，各项指标测试结果的平均值列入表 2。

(1)白噪声攻击：使用信噪比为 20 dB, 30 dB 和 40 dB 的白噪声进行攻击。

(2)低通滤波：两种语音经过通带截止频率为 6 kHz 的 Butterworth 低通滤波器处理。

(3)重采样：对两种语音进行上、下两种重采样攻击。上采样：采样率按 16–32–16(kHz)变化；下采样：采样率按 16–8–16(kHz)变化。

(4)重量化：对两种语音进行升位和降位两种重量化攻击。升位量化：携密载体语音的量化精度按 16–32–16(bit)变化；降位量化：携密载体语音的量化精度按 16–8–16(bit)变化。

(5)回声干扰：携密载体语音加入 10 ms 的回声干扰。

实验测试结果表明：

(1)本文算法对白噪声和低通滤波攻击具有较好的鲁棒性。在 40 dB 噪声攻击和低通滤波攻击下，

表 1 无攻击测试实验结果

语种	SNR_1(dB)	$PESQ_1$	SNR_2(dB)	$PESQ_2$	BER(%)	Cap(bit/s)
中文男声	21.487	3.893	13.856	4.265	0.014	100
中文女声	22.396	3.905	13.857	4.142	0.018	100
英文男声	20.015	3.868	13.856	4.161	0.015	100
英文女声	20.232	3.872	13.856	4.155	0.017	100

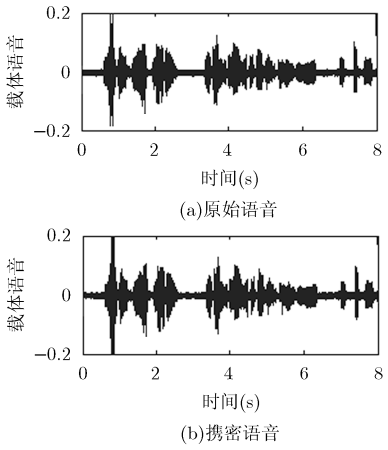

图 5 载体语音嵌入信息前后波形对比图

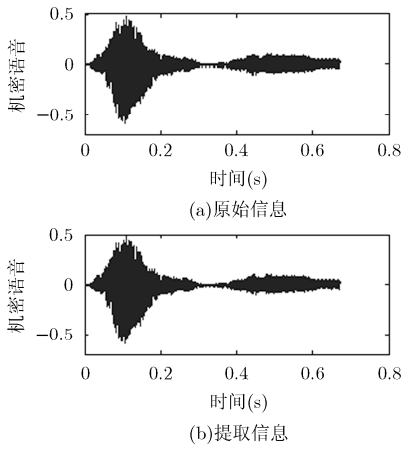

图 6 机密语音提取前后波形对比图

表 2 攻击测试实验结果

攻击方式	SNR(dB)	SNR_1(dB)	SNR_2(dB)	PESQ	$PESQ_1$	$PESQ_2$	BER(%)			
							本文算法	文献[10]	文献[11]	文献[12]
20 dB 白噪声	20	17.876	10.486	3.580	3.495	2.415	5.270	–	5.00	–
30 dB 白噪声	30	21.546	12.702	4.370	3.874	4.135	0.018	–	2.00	–
40 dB 白噪声	40	22.929	13.857	4.480	3.881	4.155	0.015	0.48	1.00	7.00
低通滤波	25.770	18.329	12.513	4.105	3.847	4.052	0.026	0.87	50.00	–
上重采样	25.680	19.386	13.856	4.500	3.866	4.276	0.013	–	5.40	0.00
下重采样	15.509	13.463	11.632	4.103	3.781	2.756	2.810	–	0.10	0.00
升量化	25.680	19.164	13.856	4.500	3.906	4.288	0.013	–	0.20	–
降量化	12.933	12.135	9.624	3.446	3.418	2.246	7.220	0.00	0.20	–
回声干扰	24.980	19.287	12.128	4.312	3.852	3.921	0.075	1.26	–	–

携密载体语音具有较高的 SNR_1 值和 $PESQ_1$ 值，提取的机密信息 SNR_2 和 $PESQ_2$ 值较高，BER 值极小，听觉效果良好，与文献[10–12]相比具有更好的鲁棒性能。在 30 dB 和 20 dB 噪声攻击下，原始语音和携密语音质量都有下降，提取的机密信息 SNR_2 降低，BER 值升高，说明较大的白噪声攻击对两种语音质量影响都很大，原始载体语音即使未隐藏有机密信息其语音质量也受损严重。可见，本文算法对抗白噪声和低通滤波这两种攻击具有较好的鲁棒性。

(2)本文算法对上采样和升量化攻击具有较好的鲁棒性，下采样和降量化攻击对算法鲁棒性有一定影响。采样改变的是语音采样点的位置，量化改变的是采样点的幅值。上采样和升量化后采样点位置和幅值基本无变化，所以载体语音质量非常好，提取的机密信息误码率较低。下采样和降量化后采样点数和采样幅值变化较大，两种载体语音的 SNR 和 PESQ 下降都较为明显，但其 PESQ 值仍在 3.5 左右，提取的机密信息 BER 值略逊于文献[10–12]。

(3)较小的回声干扰对本文算法鲁棒性基本无影响。回声干扰在 10 ms 左右时，本文算法性能非常好，说明延时较小的回声干扰对算法性能影响较小。

(4)本文算法的鲁棒性在白噪声、上采样、升量化、低通滤波和回声干扰 5 种攻击下比文献[10–12]中所述算法优越。下采样和降量化攻击时鲁棒性稍逊于文献[10–12]中算法。

5 结论

基于小波变换的信息隐藏算法根据机密信息的二进制状态调节载体语音的各级高频小波系数，从而改变语音段前后两部分的能量状态来隐藏信息，提取机密信息时通过对比语音段中前后两部分的能量大小识别机密信息，无需原始载体语音，能实现机密信息的盲提取。针对具体的应用背景，可通过调节隐藏频段、嵌入深度和语音分段长度 3 项参数平衡算法性能指标。实验及分析结果表明，该算法具有较好的隐蔽性和鲁棒性，能够对抗白噪声、低通滤波、重采用、升量化和回声干扰等多种攻击，在保证载体语音质量的条件下每一语音段内可实现 2 bit 的信息隐藏，且语音分段长度越小，小波分解级数越多，则隐藏容量越大。

参 考 文 献

[1] YANG Jun, BAI Sen, HUANG Yongfeng, *et al.* Implementation of steganography based on HOOK[J]. *Advances in Intelligent and Soft Computing*, 2012, 112(3): 133–141. doi: 10.1007/978-3-642-25194-8_16.

[2] MAZUROZYK W. VOIP steganography and its detection: A survey[J]. *ACM Computing Surveys*, 2013, 46(2): 20–26. doi: 10.1145/2543581.2543587.

[3] HUANG X P, NOBUTAKA O, ISAO E, *et al.* Reversible audio information hiding based on integer DCT coefficients with adaptive hiding locations[C]. Proceedings of the 12th International Workshop on Digital-Forensics and Watermarking (IWDW), Auckland, 2013: 376–388.

[4] 张秋余, 孙媛, 晏燕. 基于分块自适应压缩感知的可逆水印算法[J]. 电子与信息学报, 2013, 35(4): 797–804. doi: 10.3724/SP.J.1146.2012.00914.

ZHANG Qiuyu, SUN Yuan, and YAN Yan. A reversible

watermarking algorithm based on block adaptive compressed sensing[J]. *Journal of Electronics & Information Technology*, 2013, 35(4): 797–804. doi: 10.3724/SP.J.1146.2012.00914.

[5] 肖迪, 邓秘密, 张玉书. 基于压缩感知的鲁棒可分离的密文域水印算法[J]. 电子与信息学报, 2015, 37(5): 1248–1254. doi: 10.11999/JEIT141017.
XIAO Di, DENG Mimi, and ZHANG Yushu. Robust and separable watermarking algorithm in encrypted image based on compressive sensing[J]. *Journal of Electronics & Information Technology*, 2015, 37(5): 1248–1254. doi: 10.11999/JEIT141017.

[6] MOHAMMED K and ABDELLAH A. Audio watermarking with high embedding capacity based on multiple access techniques[J]. *Digital Signal Processing*, 2014, 34(1): 116–125. doi: 10.1016/j.dsp.2014.07.009.

[7] 赵学敏, 郭宇弘, 邹学强, 等. 用于版权管理的数字音频水印算法[J]. 电子与信息学报, 2011, 33(10): 2384–2389. doi: 10.3724/SP.J.1146.2011.00009.
ZHAO Xuemin, GUO Yuhong, ZOU Xueqiang, *et al*. Digital audio watermarking algorithm for media copyright management[J]. *Journal of Electronics & Information Technology*, 2011, 33(10): 2384–2389. doi: 10.3724/SP.J.1146.2011.00009.

[8] NUGRAHA R M. Implementation of direct sequence spread spectrum steganography on audio data[C]. Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, Bandung, 2011: 1–6.

[9] 邹明光, 李芝棠. 基于振幅值修改的 wav 音频隐写算法[J]. 通信学报, 2014, 35(z1): 36–40. doi: 10.3969/j.issn.1000-436x.2014.z1.008.
ZOU Mingguang and LI Zhitang. Wav-audio steganography algorithm based on amplitude modifying[J]. *Journal on Communications*, 2014, 35(z1): 36–40. doi: 10.3969/j.issn.1000-436x.2014.z1.008.

[10] 彭宏, 王珣, 王卫星. 基于音频特征的多小波域水印算法[J]. 计算机研究与发展, 2010, 47(2): 216–222.
PENG Hong, WANG Xun, and WANG Weixing. Audio watermarking approach based on audio features in multi wavelet domain[J]. *Journal of Computer Research and Development*, 2010, 47(2): 216–222.

[11] 谭良, 吴波, 刘震, 等. 一种基于混沌和小波变换的大容量音频信息隐藏算法[J]. 电子学报, 2010, 38(8): 1812–1818.
Tan Liang, Wu Bo, Liu Zheng, *et al*. An audio information hiding algorithm with high-capacity which based on chaotic and wavelet transform[J]. *Acta Electronica Sinica*, 2010, 38(8): 1812–1818.

[12] TEWARI T K, SAXENA V, and Gupta J P. A digital audio watermarking scheme using selective mid band DCT coefficients and energy threshold[J]. *International Journal of Speech Technology*, 2014, 17(4): 365–371. doi: 10.1007/s10772-014-9234-8.

[13] BAI Yinglei, ING Y S, and ZHEN Li. Blind and robust audio watermarking scheme based on SVD-DCT[J]. *Signal Processing*, 2011, 91(8): 1973–1984. doi: 10.1016/j.sigpro.2011.03.001.

[14] ALI A H. A dual transform audio watermarking algorithm[J]. *Multimedia Tools and Applications*, 2014, 73(3): 1897–1912. doi: 10.1007/s11042-013-1645-z.

[15] 刘磊, 苗启广, 石程. 面向小波域的加权分数阶微积分图像数字水印新算法[J]. 计算机应用, 2011, 31(11): 3048–3052. doi: 10.3724/SP.J.1087.2011.03048.
LIU Lei, MIAO Qiguang , and SHI Cheng. New image digital watermark algorithm with weighted fractional calculus based on wavelet coefficients[J]. *Journal of Computer Applications*, 2011, 31(11): 3048–3052. doi: 10.3724/SP.J.1087.2011.03048.

[16] HU Hwaitsu, HSU Lingyuan, and CHOU Hsienhsin. Variable-dimensional vector modulation for perceptual-based DWT blind audio watermarking with adjustable payload capacity[J]. *Digital Signal Processing*, 2014, 31(1): 115–123. doi: 10.1016/j.dsp.2014.04.014.

吴秋玲： 女，1979 年生，博士生，研究方向为信号处理、信息安全.

吴 蒙： 男，1963 年生，教授，研究方向为信息安全.