

回声隐藏的研究与实现^{*}

杨 榆, 白 剑, 徐迎晖, 钮心忻, 杨义先
(北京邮电大学信息安全中心 // 国家重点实验室, 北京 100876)

摘 要: 回声隐藏是利用音频做载体, 隐藏信息的一种信息隐藏技术。提出了基于倒谱的回声隐藏算法, 并用 matlab 实现。在此基础上, 提出了增加隐藏容量的新算法。在采样率为 44 100 Hz 条件下, 每秒能够隐藏 346 bit 信息。

关键词: 信息隐藏; 回声隐藏; 语音信号数字处理

中图分类号: TP391.41 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0050-04

信息隐藏是将保密信息隐藏于非机密载体——明文中的信息保护方法。明文可以是音频、视频、图像、文件等的任何一种数字媒体, 隐藏通过改变明文的某些参数或某部分数据实现, 并且人们察觉不到这种改变。信息隐藏同加密都是在不安全的信道中保密地传送信息的技术。两者的区别在于: 加密将明文改变为人们无法理解的密文, 以防止未经授权者获取信息; 信息隐藏虽然也通过改变明文以传送信息, 然而这种改动给明文带来的影响是人类的感官系统无法或难以察觉的, 因而非法用户意识不到携密序列隐藏了信息, 从而达到保密传输的目的。

信息隐藏技术包括: 信息分存技术、隐像技术、替声技术、数字水印技术、数字指纹、隐蔽信道, 可应用于保密通信、版权维护、防伪信息隐藏等。回声隐藏是一种基于语音的信息隐藏技术^[1]。人类听觉系统 (HAS) 十分敏锐, 能听到比周围环境低 80 dB 的噪声, 然而听觉系统也有“空穴”。人类听觉系统具有屏蔽特性, 即, 相距很短的语音 (几十 ms 以内), 幅度较弱者会被较强者遮蔽。回声隐藏利用了这个特性, 其原理是: 在原始语音——明文加入不同延迟的回声, 从而将密文嵌入明文中。在接收端, 使用延迟检测算法提取密文。

回声隐藏有很多优点: 隐藏算法简单; 算法不产生噪声, 隐藏效果好; 对同步的要求不高, 算法本身甚至可以做粗同步的工具。但它同时也存在缺陷: 当回声幅度较小时, 回声在变换域的尖峰容易被淹没。矛盾的是, 如果增大回声幅度, 则隐藏效

果又会降低。回声隐藏的一个公开问题是: 如何在回声幅度较小的情况下, 提高恢复率。因而现有大部分研究集中在对“核”的改造上^[2,3]。都提出不同的多回声“核”^[4], 总结了相关研究成果, 提出引入前向 (回声超前于原声) 和后向回声的核, 并推导它在变换域的形式, 从而说明了该方法可以提高检测率。不足的是, 这些方法的隐藏容量都不高^[4], 在采样率为 44 100 Hz 的条件下, 每秒能够隐藏 10 ~ 20 bit 数据。作者提出基于倒谱的回声检测, 结合窗函数技术, 提高了数据恢复率。在此基础上, 提出多位置隐藏算法, 提高隐藏容量, 在采样率为 44 100 Hz 条件下, 每秒能够隐藏 346 bit 信息。

1 回声隐藏算法

1.1 原 理

解隐藏算法的关键是回声延迟检测。Bender 提出复倒谱检测法。根据同态信号处理知识^[1,5,6], 信号

$$x[n] = \text{IDFT}(\ln(\text{DFT}(x[n]))) , \\ c_x[n] = \text{IDFT}(\ln(|\text{DFT}(x[n])|))$$

分别为信号 $x[n]$ 的复倒谱和倒谱信号。由隐藏算法原理可知, 携密序列等效于明文经过系统 $H[n] = 1 + \alpha \delta[n-d]$, 也称为“核” (Kemel), 的输出, 即密文 $y[n] = x[n] + \alpha \cdot x[n-d] = x[n] * H[n]$ 。利用文[6]复倒谱信号的解卷性质可得:

$$\tilde{y}[n] = \tilde{x}[n] + H[n]$$

根据计算可知, $H[n]$ 仅在回声延迟的整数倍位置

* 收稿日期: 2004-09-11

基金项目: 国家重点基础研究发展规划资助项目 (G1999035804); 北京市自然科学基金资助项目; 教育部优秀青年教师资助计划资助项目

作者简介: 杨 榆 (1978 年生), 女, 博士生; E-mail: yangelm@vip.sina.com

上有非零值。所以在信号复倒谱域中，回声延迟处会出现峰值。据此可判断延迟。

然而，为了解决复倒谱运算中的复对数多值问题，必须引入^[9]相位展开、符号校正等算法，计算复杂。与此同时，若使用同样拥有解卷性质倒谱信号，不仅计算简便，而且“核”的倒谱信号具有和复倒谱信号相同的特征。因此，作者采用了倒谱信号代替复倒谱信号检测回声。试验结果显示，该方法能获得较高的数据恢复率。

1.2 隐藏算法

为了表示二进制信息，仅需引入2个不同的延迟，为了增加隐藏的信息数，可以将原声分为多个数据段，如图1(a-c)所示，密文10110010欲隐藏在明文 $x(n)$ 中(图1(d))， $x(n)$ 经过“核”

$$h_0(n) = \tilde{q}(n) + \alpha \tilde{q}(n - N_0),$$
$$h_1(n) = \tilde{q}(n) + \alpha \tilde{q}(n - N_1)$$

分别得到明文与延迟分别为 N_0 和 N_1 的回声的叠加信号，这2个信号与0、1信号混合，最后得到输出信号。

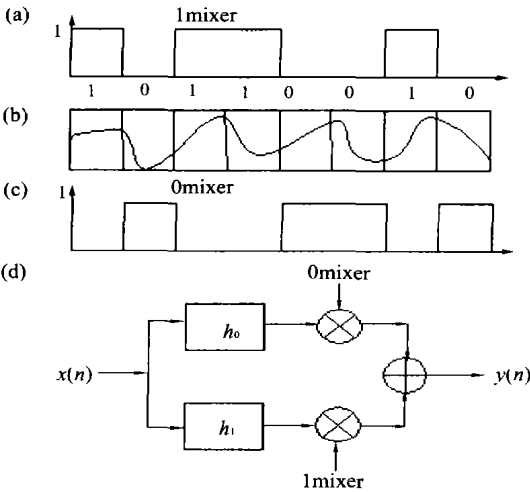


图1 隐藏原理
Fig.1 Hiding theory

1.3 提取算法

在接收端，比较携密信号在倒谱域2个特定位置处的信号幅度，便可提取保密信息，具体步骤如下(接收方已知 N_0, N_1, FRAG):

(1) 将携密信号信号 $y(n); n = 0, 1, 2, \dots, N$ 信号分段，第 i 段信号为:

$$y_i(m) = y(n) \omega(m); m = 0, 1, 2, \dots, \text{FRAG}$$
$$n = (i - 1) * \text{FRAG}, \dots, (i * \text{FRAG} - 1)$$

其中， $\omega(n)$ 为窗函数。

(2) 求取 $y_i(n)$ 的倒谱信号 $c(n)$

$$c(n) = \text{IDFT}[\ln(|\text{DFT}[y_i(n)]|)],$$

$$n = 0, 1, 2 \dots \text{FRAG}$$

其中，IDFT和DFT是信号的离散傅立叶逆变换和变换，可使用快速离散傅立叶变换(FFT)算法实现。

(3) 比较 $c(N_1)$ 和 $c(N_0)$ 的大小，若前者大于后者，判决秘密信息是1，否则是0。

2 试验结果

图2给出了在采样率为44 100 Hz、分段长度为256个采样点、延迟为6和7个采样点情况下，语音信号加了不同窗时的信息恢复率。

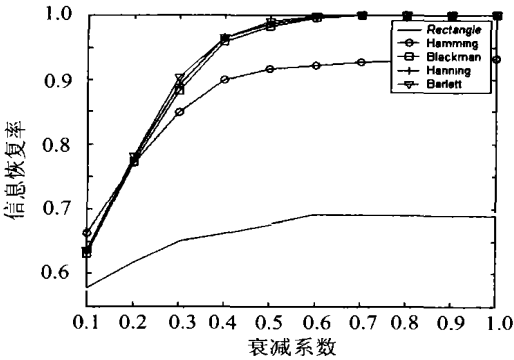


图2 窗函数对恢复率的影响
Fig.2 The influence of $\omega[n]$ upon recovery rate

结果显示，窗函数对数据恢复率有显著影响：使用Rectangle窗(以黑点标识节点的曲线)数据恢复率恒在70%以下；而使用Barlett窗(以竖线标识节点的曲线)或Hanning窗(以倒三角标识节点的曲线)时，当回声幅度仅为原声幅度的0.4时，数据恢复率就已经达到95%，当回声幅度增加到原声幅度的0.6时，数据恢复率已经达到100%。这是因为对语音信号分段处理相当于给语音信号加窗，不同类型的窗对信号功率损失的影响不同，从而显著影响了信息恢复率。

3 算法的改进——提高隐藏容量

该算法在语音信号中隐藏信息时，按照44.1 kHz采样、256个样点分段长度、6和7个采样点延迟的参数，1 s只能隐藏173 bit信息，为提高隐藏容量，作者对算法进行改进。原处理中，每个分段隐藏1 bit数据，引入2个延迟偏置，如果每个分段处理2 bit的数据，那么隐藏容量就能加倍。为此，需要引入4个延迟偏置。更改隐藏步骤为：

(1) 获取保密信息 $I(m) = i; i = \{0, 1\}, m = 0, 1, 2, \dots, M$ ，明文 $x(n); n = 0, 1, 2, \dots, N$ ，和延迟信号(d_i)

$$d_i(n)=\begin{cases}0 & n<N_i \\ x(n-N_i) & N_i\leq n\leq N_i+N-1\end{cases}$$
$$i=0,1,2,3$$

(2) 将明文分段并混入回声。

$$x'(n)=x(n)+\alpha*d_j(n);$$
$$n=(i-1)*FRAG\cdots(i*FRAG-1),$$
$$j=I(i)I(i+1)$$

更改信息提取步骤为：

将携密信号 $y(n)$ 分段为 $y_i(n)$, 计算其倒谱信号 $c(n)$, 找出 $c(N_i); i=0,1,2,3$ 中幅度最大者, 判决出隐藏信息。即, 若 $c(N_3)$ 幅度最大, 则回声延迟为 N_3 , 根据隐藏算法, 此分段对应的保密信息为：
 $I(i)=1, I(i+1)=1$ 。

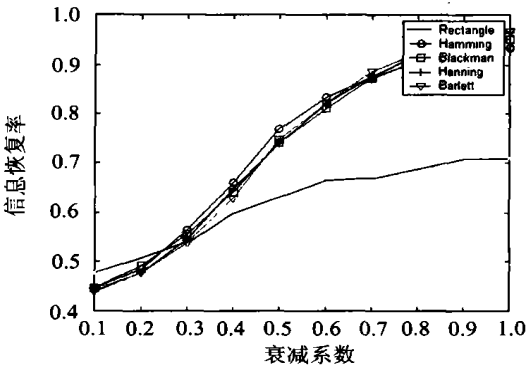


图 3 改进算法的恢复率

Fig 3 The recovery rate of the modified method

算法修改后的测试结果如图 3 所示, 数据在采样率为 44 100 Hz、分段长度为 256 个采样点、延迟为 5、6、7、8 个采样点条件下获取。可以看出：使用 Barlet 窗（以竖线标识节点的曲线）或 Hanning 窗（以倒三角标识节点的曲线）时的数据恢复率仍然较其它情况高；恢复率随着回声幅度增

强而提高, 当回声初始幅度衰减系数高于 0.7 时, 恢复率高于 90%, 满足使用要求。

4 结 论

回声隐藏是一种信息隐藏技术, 作者提出了通过在倒谱域中比较信号回声位置处幅度值强度来恢复信息的方法, 用 matlab 实现并测试了数据。算法在一秒钟内隐藏 173 bit (采样率为 44 100 Hz) 信息, 恢复率能达 100%, 并且, 由于回声距原声的延迟在 0.1 μs 左右, 所以隐藏效果良好。在此基础上, 作者使用多延迟位置的方法提高了信息隐藏容量。然而, 算法依赖于倒谱域信号幅度, 抗噪声性能不强。因此, 在后续研究中, 如何提高算法抗噪声能力以及如何选择参数, 达到隐藏容量、隐藏效果、抗噪声能力的平衡, 将成为重点。

参考文献:

[1] XIN L, YU H H. Transparent and robust audio data hiding in cepstrum domain [C] . Multimedia and Expo, IEEE International Conference, 2000, 1: 397—400.

[2] HYEM O O, HYUN W K, JONG W S. Transparent and robust audio watermarking with a new echo embedding technique [J] .Multimedia and Expo, 2001: 317—320.

[3] HYEN O O, JONG W S, JIN W H, et al. New echo embedding technique for robust and imperceptible audio watermarking [J] . Acoustics, Speech, and Signal Processing, 2001, 3: 1341—1344.

[4] KIM H J, CHOI Y H. A novel echo-hiding scheme with backward and forward kernels[J] . Circuits and Systems for Video Technology, 2003, 13: 885—889.

[5] BENDER W, GRUHL D, MORIMOTO N. Techniques for data hiding[J] . IBM Systems J, 1996, 35(3&4) .

[6] 姚天任, 孙洪. 现代数字信号处理[M] . 武昌: 华中理工大学出版社, 1999: 171—180.

Research and Realization of Echo Data Hiding

YANG Yu, BAI Jian, XU Ying hui, NIU Xin xin, YANG Yi xian

(State Key Laboratory //Information Security Center, Beijing University of Posts &Telecomm, Beijing 100876, China)

Abstract: With audio host, echo data hiding is one of information hiding technique. Puts forward an echo data hiding arithmetic without cepstrum and implement it using matlab. In addition to it, advances a new arithmetic increasing capacities of echo data hiding. On the condition of 44.1 kHz sample rate, the capacity of the new arithmetic reaches 346 bps.

Key words: information hiding; echo data hiding; digital processing of audio signal