信息隐藏与检测算法的特性分析

钮心忻, 杨义先
(北京邮电大学信息安全中心, 北京 100876)

摘 要: 本文从系统模型的角度研究了信息隐藏与检测的问题, 提出了用参数估计理论来衡量信息提取算法的优劣. 同时, 用信息隐藏中常用的两种算法和四种应用环境为例, 推导了参数估计的方差下限, 并且用仿真结果验证了理论结果, 同时得到了对应的信息提取算法为最佳估计算法的结论.

关键词: 信息隐藏与检测; 参数估计; CRLB (Cramer Rao Lower Bounds)
中图分类号: TN919.3 文献标识码: A 文章编号: 0372-2112 (2002) 07-0952-04

Performance Analysis on the Algorithms of Information Hiding and Extracting

NIU Xin-xin, YANG Yi-xian
(*Information Security Center, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: The problem of information hiding and extracting is studied in the perspective of system model in this paper. An approach is proposed to measure the performance of information extracting algorithms by using the estimation theory. The Cramer Rao Lower Bounds (CRLB) are derived for four algorithms of information extracting and the simulation results are given to corroborate the analysis.

Key words: information hiding and extracting; parameter estimation; CRLB

1 引言

在信息技术和网络技术飞速发展的今天, 我们面临大量信息的数字化传播. 一方面信息的传播存在安全保密的问题, 另一方面数字产品的传播和复制存在版权保护的问题. 信息隐藏技术就是在这样的需求情况下应运而生的. 信息隐藏的一个方面是信息伪装技术, 就是在传统加密技术的基础上增加一层伪装色, 比如将机密信息经过加密后, 隐藏在一个普通的、可懂的信息中进行传输, 如声音、图像或者视频信号, 因为这些信号具有较大的信息冗余度, 利用这些冗余度就可以隐藏一些信息, 而隐藏了信息后的这些载体信号又没有严重的降质, 因此不易引起攻击者的怀疑, 可以保证信息安全地到达接收端. 信息隐藏的另一方面就是数字水印技术, 在当前数字信息的传播和复制日益容易的情况下, 如何保证一个具有知识产权的数字产品能够得到版权保护, 不被非法复制, 这就是数字水印技术需要解决的问题.

不论是信息伪装技术和数字水印技术, 其核心就是一个信息的隐藏和提取. 在这些方面的研究过程中, 提出了大量的算法, 这些算法是针对不同的应用环境和不同的应用对象而设计的. 信息的加载有基于时域的, 也有基于变换域的; 信息的提取有需要精确恢复的, 和不需要精确恢复的; 信息提取时有需要原始信号的, 和不需要原始信号的等等. 在目前发表的文献中[1~6], 大部分是针对特定的应用和特定的要求而提出特定的算法, 对算法的信息加载、信息提取过程进行描述, 并且试验该算法抵御各种攻击和破坏的能力. 目前的研究中只有为数不多的文献从系统模型的角度研究信息的加载和提取[7]. 本文将从信号分析和参数估计的角度研究信息的加载与提取.

本文首先建立了一个信息隐藏与检测系统的模型, 在这个模型中, 概括了通常使用的一些信息隐藏和提取的基本模型. 然后, 对参数估计理论进行了简单的介绍, 主要介绍了最小方差无偏估计的概念和其下限值 CRLB(Cramer Rao Lower Bound) 的产生. 第四部分针对目前信息隐藏的两种算法推导出了参数提取时的 CRLB 值, 每一种算法中都考虑了两种不同的应用环境. 第五部分通过大量的仿真结果对我们导出的估计方差的下限 CRLB 值进行了验证.

2 信息隐藏与检测系统模型

首先, 我们给出一个信息隐藏与检测的系统模型(图 1), 它包括两个模块——信息加载模块和信息提取模块, 其中 S 为载体信号, W 为需要隐藏的信息, K 为信息加载的密钥. 加

收稿日期: 2001-03-30; 修回日期: 2001-07-12
基金项目: 国家自然科学基金(No. 60073049); 国家重点基础研究发展规划项目(No. G1999035805); 高等学校骨干教师资助计划

图 1　信息隐藏和检测的系统模型

载了信息的载体信号变为 X, 通过信道后, 由于受到信道的干扰或者各种变换处理, 接收端收到的信号为 Y. 在接收端, 从信号 Y 中试图提取出所隐藏的信息 W', 根据提取算法的不同, 可能已知(或未知)密钥 K, 已知(或未知)原始信号 S, 或者已知 S 的微小变形 S'.

在这里, 把信息隐藏和数字水印技术综合为图 1 所示的系统模型. 其中, 对于正常接收者而言, 密钥 K 是已知的, 而对于网上的攻击者或者监控者而言, 密钥 K 是未知的. 对于某些提取算法, 需要精确的原始信号 S, 有些可能只需要不太精确的原始信号 S', 或者根本不需要原始信号. 对于提取的信号 W', 在某些应用场合可能需要精确恢复, 比如通过信息的伪装传递短信息; 某些场合可能需要不太精确的恢复即可, 比如可视数字水印, 只需要提取出的可视水印具有原水印的基本信息, 通过人眼可以判断水印的存在即可; 某些场合可能只需判断水印的存在与否, 比如随机数字水印, 只需要将提取出的水印与原始水印进行相关计算, 由其相关性大小判定水印是否存在. 因此, 图 1 所示的隐藏和检测模型可以包容目前研究的基本方向.

3　参数估计理论

现代估计理论[8]在信号处理中有着很广泛的应用, 如雷达、声纳、语音、图像、通信、控制等领域, 它主要应用于参数的提取, 就是从一串数字序列中提取出一些特定的参数. 用数学方式表示就是, 已知 N 点数据, 它们是基于一个未知参数 θ 的, 要设计一个估计算法 g, 从中估计出参数, $\theta = g(x[0], x[1], \cdots, x[N])$. 对同一个问题可能会有多种不同的估计算法, 如何评价一个估计算法的好坏, 这就是估计理论需要解决的问题.

在估计理论中, 参数是被淹没在观察到的数据中的, 而观察到的数据是由它的概率密度函数(PDF)来描述的, 可以想象, 如果观察数据的概率密度函数完全与参数无关, 那么提取出的参数是毫无准确性可言的, 因此观察数据的 PDF 是被提取的参数的函数. 这样的概率密度函数又称为似然函数, 当这样一个正态分布曲线窄而陡时, 说明从观察数据中估计参数比较精确, 而当正态分布曲线宽而较平坦时, 说明从这些数据中估计参数的误差比较大. 因此正态分布曲线的陡度可以用函数对参数 θ 的二次导数的负值来衡量, 它又称为对数似然函数的曲率.

定理 **1(CRLB 定理)**　假设概率密度函数满足正则条件, 即对所有的 θ, 满足 $E[\frac{\partial \ln p(x;\theta)}{\partial \theta}] = 0$, 那么任何一个无偏估计算法的方差满足 $\mathrm{var}(\theta) \geq \frac{1}{-E[\frac{\partial^2 \ln p(x;\theta)}{\partial \theta^2}]}$.

这个定理给出了任何一个估计算法所能达到的最小方差. 因此, 用 CRLB 可以衡量一个估计算法与最小方差的差别, 以此来比较各种估计算法的性能[9].

4　信息检测特性分析

在信号的幅值上叠加信息, 无论是在时域(或空间域)还是在变换域, 常见的叠加方式有两种, 一种是直接在信号的幅值上叠加, 一种是根据信号的幅度按比例叠加, 即: $s(t) + \alpha w(t)$ 和 $s(t)[1 + \alpha w(t)]$, 其中, $s(t)$ 为信号的幅值, $w(t)$ 为需要叠加的信息, α 为一个可调参数. 通常后一种方式较好, 它是根据信号的大小来携带信息, 信号强, 可以多携带一些信息, 而信号弱, 就可以少带一些信息. 而第一种方式则可能造成当信号强时没有充分利用, 而信号弱时所携带的较强信息对原始信号产生较大的干扰.

在信息的隐藏与检测中, 如何从携带信息的载体中提取出信息, 或者根据提取出的信息判断是否存在隐藏的信息, 这些都要根据特定的隐藏算法来设计提取算法, 可能存在一种或者多种提取算法, 算法不同, 提取信息的准确程度也不同. 但是不管什么样的提取算法, 它们所能达到的最小误差由 CRLB 决定.

本文将根据参数估计理论, 推导出几种信号提取模型的 CRLB.

4.1　直接叠加

已知原始信号, 信号模型可以表示为:

$$\begin{cases} f_1(t) = s(t) \\ f_2(t) = s(t) + \alpha w(t) + n(t) \end{cases}$$

其中: $s(t)$ 为原始载体信号; $w(t)$ 为需要隐藏的信号(如 0, 1 比特串); α 为可调参数; $n(t)$ 代表隐藏了信息的载体通过信道时所受到的干扰, 可以假设为高斯白噪声; $f_2(t)$ 表示接收端收到的信号, 即图 1 中的 Y 信号, 而 $f_1(t)$ 表示提取时需要的原始载体信号, 即图 1 中的 S 信号.

从参数估计理论, 可以推导出这样一个信号模型的 CRLB. 已知 $n(t)$ 为白色高斯噪声, 问题变为从接收到的 $f_2(t)$ 中估计出 $w(t)$, 其中 $s(t)$ 和 α 为已知. $n(t)$ 的概率密度函数为

$$p(f_2(t); w(t)) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp[-\frac{1}{2\sigma^2}(f_2(t) - s(t) - \alpha w(t))^2]$$

对数似然函数为

$$\ln p(f_2(t); w(t)) = K - \frac{1}{2\sigma^2}(f_2(t) - s(t) - \alpha w(t))^2$$

求其两阶偏导数, 由定理 1 可推出最小估计方差 CRLB 为

$$\mathrm{var}[\hat{w}(t)]_{\mathrm{CRLB}} = \sigma^2/\alpha^2$$

4.2　间接叠加

已知原始信号, 信号模型可以表示为:

$$\begin{cases} f_1(t) = s(t) \\ f_2(t) = s(t)[1 + \alpha w(t)] + n(t) \end{cases}$$

已知 $n(t)$ 为白色高斯噪声, 问题变为从接收到的 $f_2(t)$ 中估计出 $w(t)$, 其中 $s(t)$ 和 α 为已知. 通过与前面类似的推导, 可以得到参数估计的 CRLB 为:

$$\mathrm{var}[\hat{w}(t)]_{CRLB}=\sigma^2/\alpha^2 s^2(t)$$

4.3 直接叠加(原始信号受干扰)

信号模型为:

$$\begin{cases} f_1(t)=s(t)+n_1(t) \\ f_2(t)=s(t)+\alpha w(t)+n_2(t) \end{cases}$$

这里,原始信号受到干扰的影响,接收端做为参考信号的只能是$f_1(t)$而非$s(t)$,由于参考信号受到干扰的影响,造成参考信号不准确.假设由于干扰$n_1(t)$的影响而产生的估计偏差由$w_1(t)$来代表,因此上面的信号模型可以改写为下式:

$$\begin{cases} f_1(t)=s(t)+\alpha w_1(t)+n_1(t) \\ f_2(t)=s(t)+\alpha w_2(t)+n_2(t) \end{cases}$$

其中$w_1(t)$表示由于$n_1(t)$引起的信息偏差;$w_2(t)$表示由于$n_2(t)$引起的信息偏差;而最后提取的信息则可以表示为$w(t)=w_2(t)-w_1(t)$.

假设$n_1(t)$和$n_2(t)$为相互独立、不相关的白色高斯噪声,因此它们的联合概率密度为两个概率密度的乘积:

$$\begin{aligned} &p(f_1(t),f_2(t);w_1(t),w_2(t)) \\ &=p(f_1(t);w_1(t))p(f_2(t);w_2(t)) \\ &=\frac{1}{\sqrt{2\pi\sigma_1^2}}\exp\left[-\frac{1}{2\sigma_1^2}(f_1(t)-s(t)-\alpha w_1(t))^2\right] \\ &\quad\cdot\frac{1}{\sqrt{2\pi\sigma_2^2}}\exp\left[-\frac{1}{2\sigma_2^2}(f_2(t)-s(t)-\alpha w_2(t))^2\right] \end{aligned}$$

它是两个参数$w_1(t)$和$w_2(t)$的函数,而需要估计的参数$w(t)$是它们的函数$w(t)=w_2(t)-w_1(t)$,利用估计理论中多参数估计的 CRLB 公式和参数的函数变换公式[8],可以得到以下推导.这里把被估计的参数定义为一个矢量$\theta=[w_1(t),w_2(t)]^T$. Fisher 信息矩阵定义为$[I(\theta)]_{ij}=-E\left[\frac{\partial^2\ln p}{\partial\theta_i\partial\theta_j}\right]$,通过推导,可以得到 Fisher 信息矩阵为$I(\theta)=\begin{bmatrix}-\alpha^2/\sigma_1^2 & 0\\ 0 & -\alpha^2/\sigma_2^2\end{bmatrix}$,参数估计的方差下限 CRLB 为$\mathrm{var}(\theta)_{CRLB}=I(\theta)^{-1}$,而最终要估计的参数是$w(t)=w_2(t)-w_1(t)$,它是θ的函数,写为$w(t)=g(\theta)$.根据对于参变量函数的估计公式:$\mathrm{cov}(\hat{g})\geq\frac{\partial g(\theta)^T}{\partial\theta}I^{-1}(\theta)\frac{\partial g(\theta)^T}{\partial\theta}$,而$\frac{\partial g(\theta)}{\partial\theta}=[-1,1]$,可以得出当参考信号存在噪声干扰时,隐藏信号的估计方差下限,即$\mathrm{var}[\hat{w}(t)]_{CRLB}=(\sigma_1^2+\sigma_2^2)/\alpha^2$.

4.4 间接叠加(原始信号受干扰)

信号模型为:

$$\begin{cases} f_1(t)=s(t)+n_1(t) \\ f_2(t)=s(t)[1+\alpha w(t)]+n_2(t) \end{cases}$$

这里,假设原始信号受到噪声$n_1(t)$的影响,接收端做为参考信号的只能是$f_1(t)$而非$s(t)$,由于参考信号受到干扰的影响,造成参考信号不准确.与上类似,假设由于干扰$n_1(t)$的影响而产生的估计偏差由$w_1(t)$来代表,因此上面的信号模型可以改写为:

$$\begin{cases} f_1(t)=s(t)[1+\alpha w_1(t)]+n_1(t) \\ f_2(t)=s(t)[1+\alpha w_2(t)]+n_2(t) \end{cases}$$

其中$w_1(t)$表示由于$n_1(t)$引起的信息偏差,$w_2(t)$表示由于$n_2(t)$引起的信息偏差,而最后需要提取的信息为$w(t)=w_2(t)-w_1(t)$.

同样假设$n_1(t)$和$n_2(t)$为相互独立、不相关的白色高斯噪声.与上面类似,同样可以推导出参数估计$w(t)$的方差下限:

$$\mathrm{var}[\hat{w}(t)]_{CRLB}=(\sigma_1^2+\sigma_2^2)/\alpha^2 s^2(t)$$

5 仿真结果

在这里,分别对在时域和小波变换域中的两种信息叠加算法进行了仿真,仿真中又分别考虑了上面四种情况.仿真中,我们采用一段 2 秒的语音信号做为载体信号.需要隐藏的信息为一串比特流.2 秒的语音信号以 8kHz 的采样率采样,叠加的比特流的长度分别为 100 比特和 1000 比特.在实验中,这些比特流是随机产生的.

5.1 直接叠加算法(参考信号无噪音)

首先,比较在时域和小波变换域采用直接叠加算法隐藏信息的情况.在算法中,我们对时域中的语音信号找出其幅度绝对值最大的前 J 个点,在其上叠加 J 个信息比特,即$x(i)=s(i)+\alpha w(i),(i=1,\cdots,J)$,由于叠加了信息,产生了一定的信噪比.另外,当隐藏了信息的语音进行传输时,受到信道噪声的影响,因此接收端收到的信号为$y=x+n$,接收端从y和原始信号s中提取出信息比特w,$w(i)=[y(i)-s(i)]/\alpha$.

在小波变换域的信息隐藏也采用类似的方法,首先将原始语音变换到小波域,在小波域中找出其幅度绝对值最大的前 J 个点,叠加 J 个信息比特。而信道噪声是对时域信号的影响,因此在接收端是分别将接收信号和原始信号变换到小波域后再进行提取的。

在前一节已经推导了直接叠加算法,信息提取的估计误差下限 CRLB 为$\mathrm{var}[w(t)]_{CRLB}=\sigma^2/\alpha^2$.图 2 中画出了 CRLB 随信噪比的变化曲线,图中"*"给出了 100 次随机仿真的平均估计方差.应注意,实验得到的估计方差与 CRLB 是非常一致的。图 2 显示了在时域和小波域隐藏$J=100$比特的结果,另外还对在时域和小波域隐藏$J=1000$比特进行了仿真,其结果与图 2 近似。可以看出,隐藏的信息比特的多少,不影响估计的方差,但是它们将影响原始语音信号的信噪比,当然隐藏信息越多的话,对载体信号的影响越大。

5.2 间接叠加算法(参考信号无噪音)

这里,将间接叠加算法应用在语音信号的时域和小波域中,进行信息的隐藏.在仿真中,分别在时域中和小波域中找出幅度绝对值最大的前 J 个点,在这些点上叠加信息比特,即$x(i)=s(i)[1+\alpha w(i)],(i=1,\cdots,J)$.在信道中同样会受到噪声的干扰,因此在接收端收到的信号为$y=x+n$,接收端从y和原始信号s中提取出信息比特w,$w(i)=[y(i)/s(i)-1]/\alpha$.

对算法进行了 100 次随机仿真,得到了在不同信噪比情况下的平均估计方差,并将其与 CRLB 相比较.因为在 CRLB 的理论结果中,最小方差除了与信噪比和α有关外,还与所叠加信息那一点的幅度值有关,因此分别给出了几个不同点的 CRLB 和实验结果.图 3 中给出了在最大幅度点隐藏信息

的特性, 其中虚线为在时域中叠加信息的 CRLB, “ * ” 为相应的仿真结果, 实线为在小波域中叠加的 CRLB, “ o” 为相应的仿真结果. 同时还注意到, 时域结果比小波域结果估计的方差要大, 这点说明了同样情况下在小波域中隐藏信息受到噪声的干扰较小, 可以较精确地提取出隐藏的信息. 图 4 给出了在第 $J/2$ 点隐藏信息的特性, 我们知道, 从第一点、第 $J/2$ 点到第 J 点, 载体信号的幅值是逐渐降低的, 因此在越小的幅度上隐藏信息, 其提取后的误差越容易受到噪声的影响. 从图 3 和图 4 可以注意到, 参数估计的方差越来越大. 同时也注意到, 仿真结果与理论分析比较吻合.

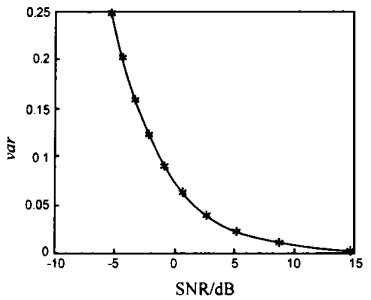

图 2　CRLB 与仿真结果 (100 点, 时域和小波域)

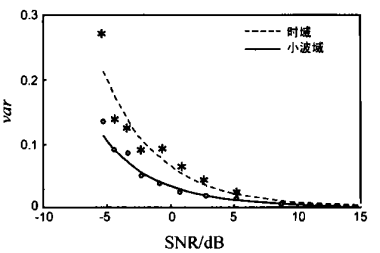

图 3　在最大点隐藏的特性

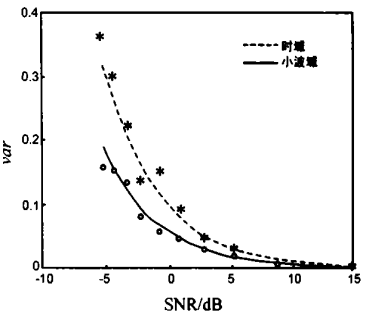

图 4　在第 $J/2$ 点隐藏的特性

5.3　间接叠加算法(参考信号有噪音)

在这一组实验中, 同样采用在时域和小波变换域隐藏信息, 并采用间接叠加算法, 但它与上面一组实验不同的地方在于, 在这里, 参考信号受到少量噪声的干扰. 比如在实际应用中, 接收端需要一个原始参考信号进行运算, 但是这个参考信号可能是原始信号的一个微小变形, 如原始信号受到线路上的噪声影响, 或者原始信号经过有损压缩后的重建等等. 因此这里用一个高斯白噪声近似这个原始信号受到的影响. 前一节已经推导出了在这种情况下的最小估计方差 CRLB, 这里将实验结果与理论结果进行了比较. 在有噪声存在的情况下, 采用与图 3、4 同样的条件, 得到了和图 3、4 几乎一样的曲线, 这里略去. 从而从实验上验证了理论推导的正确性.

在以上实验中, 我们通过大量数据的仿真, 得到了一批参数估计的方差, 与理论推导的 CRLB 相比较, 得到了较为一致的结果, 验证了理论结果的正确性, 同时说明这样的提取算法达到了理论上的最佳值, 是最佳估计算法. 而且同样的隐藏和提取算法, 在小波域中比在时域中应用可以得到更好的隐藏和提取效果.

6　结论

本文将参数估计理论应用到信息隐藏的提取问题中, 分析了两种隐藏算法在四种应用环境下的估计方差的下限, 并且比较了在时域和小波变换域中隐藏信息的特性. 仿真结果验证了理论推导的正确性, 并且证明了这样的提取算法达到了理论上的最佳值, 是最佳估计算法. 本文的意义在于将估计理论与信息隐藏和检测的问题相联系, 为设计最佳隐藏算法和检测算法提供了衡量准则和依据.

参考文献:

[1] I J Cox, J Kilian, F T Leighton, T Shamoon. Secure spread spectrum watermarking for multimedia [J]. IEEE Trans. on Image Processing, 1997, IP-6(12): 1673– 1687.

[2] N F Johnson, S Jajodia. Exploring steganography: seeing the unseen [J]. Computer, 1998, 31(2): 26– 34.

[3] W Bender, D Gruhl, N Morimoto, A Lu. Techniques for data hiding [J]. IBM System Journal, 1996, 35(3&4): 313– 336.

[4] M D Swanson, B Zhu, A H Tewfik, L Boney. Robust audio watermarking using perceptual masking [J]. Signal Processing, 1998, 66: 337– 355.

[5] 钮心忻, 杨义先. 基于小波变换的数字水印隐藏与检测算法 [J]. 计算机学报, 2000, 23(1): 21– 27.

[6] 陈明奇, 钮心忻, 杨义先. 基于小波变换及矢量量化的隐像术 [J]. 计算机研究与发展, 2001, 38(2): 199– 203.

[7] F Hartung, M Kutter. Multimedia watermarking techniques [J]. Proceedings of the IEEE, July, 1999, 87(7): 1079– 1107.

[8] S M Kay. Fundamentals of Statistical Signal Processing: Estimation Theory [M]. New Jersey: PTR Prentice Hall, 1993.

[9] Xinxin Niu, P C Ching, Y T Chan. Wavelet based approach for joint time delay and Doppler stretch measurements [J]. IEEE Trans. on Aerospace and Electronic Systems, 1999, 35(3): 1111– 1119.

作者简介:

钮心忻　女, 1963 年生于北京市, 1988 年在北京邮电大学获信号与信息处理专业硕士学位, 1997 年在香港中文大学获信号与信息处理专业博士学位, 现为北京邮电大学副教授, 主要研究领域为信息隐藏与数字水印、信息安全、软件无线电等.

杨义先　男, 1961 年生于四川省盐亭县, 1988 年在北京邮电大学获信号与信息处理专业博士学位, 现为北京邮电大学教授, 博士导师, 长江学者特聘教授, 全国政协委员, 主要研究领域为现代密码学、计算机网络与信息安全、信息伪装与数字水印、移动通信安全等.