数字水印的信道容量研究综述

王 颖 李象霖
(中国科学院研究生院信息安全国家重点实验室 北京 100049)

摘 要 该文对数字水印信道容量的研究结果进行了分析总结。文中介绍了作为基本通信系统的水印、作为边信息的水印、利用脏纸编码的水印及安全水印的信道容量。通过对水印信道容量的分析，得出了对水印的嵌入和检测算法研究具有指导意义的结论。

关键词 数字水印，信道容量，通信模型，边信息，游戏理论
中图分类号：TP391 **文献标识码**：A **文章编号**：1009-5896(2006)05-0955-06

An Overview of the Capacity of Digital Watermarking

Wang Ying Li Xiang-lin
(*Information Security State Key Laboratory*,*The Graduated School of the Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract The diversified researches of capacity of digital watermarking are summarized in this paper. The capacity of watermarking as a basic communication system, the capacity as side information, the capacity using dirty paper encoding and the capacity of security watermarking are introduced. An effective conclusion for designing the arithmetic of embedding and detecting is found by analysis the capacity.

Key words Digital watermarking, Channel capacity, Model of communication, Side information, Game theory

1 引言

数字水印技术因其在知识版权保护、认证等方面的重要应用价值，已成为信号处理领域最热门的研究课题之一[1]。随着研究的深入，数字水印的理论模型也得到了逐步的完善。数字水印系统本质上可以看成是一种通信系统，它是从水印嵌入端传输信息到水印接收端，水印本身是这个系统传输的信息，载体对象被看成为信道，故可将水印系统与传统的通信模型进行匹配，并用通信理论分析水印系统的性能。衡量通信系统性能的一个关键性指标为信道容量，即单位时间内信道上所能传输的最大信息量，它给出了通信系统传输信息的理论极限。对于水印系统，信道容量是指当存在攻击时一幅数字作品所能加载的最大信息量。很多研究者[2-9]基于通信理论分析水印系统模型，对水印信道容量进行了研究，本文对这方面的诸多研究成果进行了归类研究，并分析了各种典型的水印算法容量。水印容量的分析总结对水印结构研究，对水印嵌入算法设计及水印攻击算法设计具有指导作用。

目前有两种基于通信系统结构的水印模型，一种是基本水印模型(如图 1 所示)，其中载体对象被看成纯粹的噪声。本文第 2 节采用经典信息论对这类模型水印容量进行了分析；另一种是仍将载体对象看成噪声，但这个噪声给信道编码器提供边信息，即基于边信息水印系统模型，如图 2 所示。由于这种水印系统显示了较好的性能，所以基于这种模型的容量理论分析和算法较多。典型的利用 Costa 脏纸信道分析具有边信息的数字水印信道容量，在第 3 节和第 4 节中介绍；基于游戏理论分析的水印信道容量在第 5 节中介绍；第 6 节对全文进行总结。

2004-12-07 收到, 2005-05-08 改回
国家 863 计划项目(2003AA144080)资助课题

2 基本模型的水印容量

根据信息论[10]，任一有扰离散信道中，若 X 为信道中传输的信息，Y 为接收端信号，则该信道的信道容量为

$$\begin{aligned} C &= \max_{P_X(x)} I(X,Y) \\ &= \max_{P_X(x)} [H(Y) - H(Y/X)] \\ &= \max_{P_X(x)} [H(X) - H(X/Y)] \end{aligned} \tag{1}$$

式中 $P_X(x)$ 为信号 X 的概率分布函数，$I(X,Y)$ 为 X ,Y 间的互信息，$H(Y)$ 为信号 Y 的熵，$H(Y/X)$ 为条件熵，即 X 被选定后，Y 的期望熵。

基本数字水印系统模型与一般性的有扰离散信道类似，可根据式(1)计算得到扩频谱水印等基本水印模型系统的信道容量 C 。扩频谱(Spread Spectrum，SS)水印[11]是提出最早的并得到广泛公认的一种水印的嵌入方法，它是一种典型的基本数字水印系统。假设原始图像 X 服从均值为 0，方差为 σ_X^2 的高斯分布$(0,\sigma_X^2)$，攻击噪声 N 服从均值为 0，方差为 σ_N^2 的高斯分布$(0,\sigma_N^2)$，水印信号 W 也是高斯分布 $(0,\sigma_W^2)$。则根据式(1)中加性高斯白噪声(Add White Gaussian Noise，AWGN)信道的信道容量理论可得扩频水印信道容量表达式[4]：

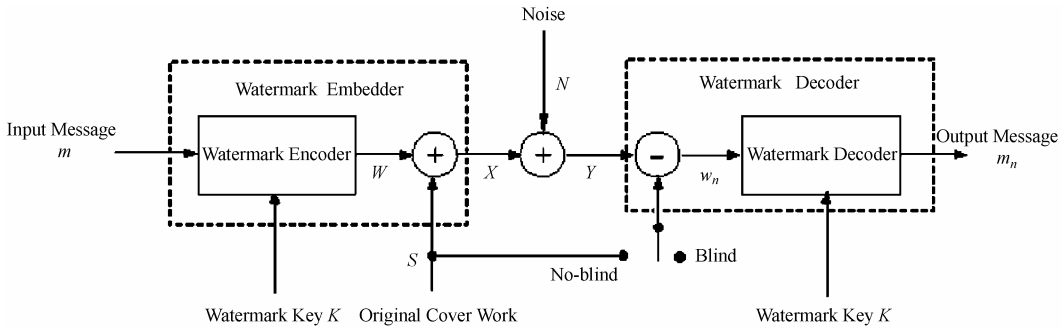

图 1 由通信模型映射而来的基本水印模型

Fig. 1 Basic watermarking model mapped into communication model

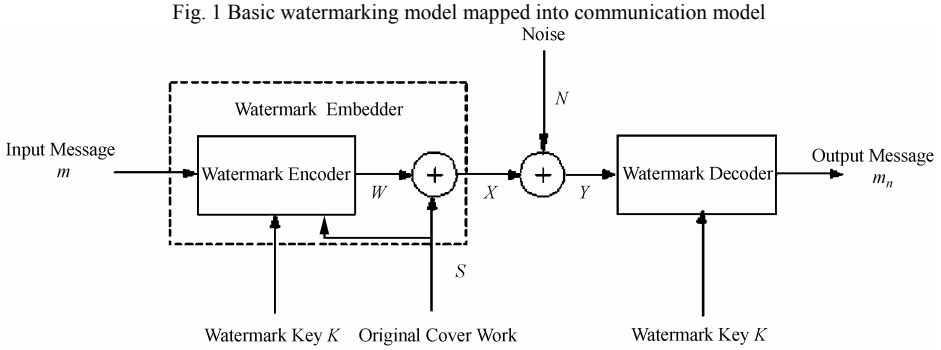

图 2 具有边信息的水印模型

Fig. 2 Watermarking model with side information

$$C_{\text{No-blind}}^{\text{SS}} = \frac{1}{2}\log_2\left(1+\frac{\sigma_W^2}{\sigma_N^2}\right) \tag{2}$$

$$C_{\text{Blind}}^{\text{SS}} = \frac{1}{2}\log_2\left(1+\frac{\sigma_W^2}{\sigma_X^2+\sigma_N^2}\right) \tag{3}$$

在以上两式中，当 $\sigma_X^2 >> \sigma_W^2$ 和 $\sigma_X^2 >> \sigma_N^2$ 时，在水印嵌入和遭到攻击时可保证原始信号的质量。可以看出，遭到 AWGN 攻击时，盲 SS 水印系统的性能主要由 DWR = $10\lg\sigma_X^2/\sigma_W^2$ [dB](式中，DWR 为原始信号与水印信号的功率比)决定。相反，遭到 AWGN 攻击时，非盲水印系统的性能完全独立于原始载体信息 X，它的性能主要由 WNR = $10\lg\sigma_W^2/\sigma_N^2$ [dB](式中，WNR 为水印噪声比)决定。由于非盲水印在水印提取时可利用原始信号的信息，则盲水印容量往往小于非盲水印容量。

3 带有边信息的信道容量

上节中介绍的基本水印模型在水印编码和解码过程中忽略了原始载体信号的信息，本节将介绍带有辅助信息的嵌入和检测的水印模型，即具有边信息的水印模型[12,13](如图 2 所示)，它具有更大的应用潜力。在这个模型中编码器将原始载体信号作为边信息，从而减少原始载体信号对水印系统性能的影响。这类信道包括脏纸信道、应用乘法噪声、随机滤波量化或其它类型的非加性失真等。Gel fand和Pinsker[14]阐明这类信道的水印信道容量为

$$C = \max_{P_{\text{SUX}}}\left[I(U;Y)-I(U;S)\right] \tag{4}$$

式中 S 是在传输器中已知的边信息的值，是与编码方式相独立的；U 是一个辅助变量，它是根据消息 m 的分布及 S 对编码方式的影响来确定的；X 是传输信号中的一个元素，一般来说它是 S 和 U 的函数，即 $X = f(U,S)$；P_{SUX} 是 S，U，X 等 3 个变量的联合概率分布。

为了理解式(4)，必须了解概率分布 P_{SUX}，它完全由 S 的分布、消息 m 的分布及编码方式确定。然而，S 的分布是作为信道的一个部分，可以假定消息 m 是符合均匀分布的，这样在公式中的最大化是指在 m 所有可能的编码方式中 P_{SUX} 取得最大。可以看出，利用式(4)很难获得一般边信息信道容量的解析解。1983 年Costa提出的脏纸信道[15]与具有边信息的盲检测水印系统几乎是完全一致的。而且在假设信道攻击为加性白噪声情况下，可获得边信息水印系统信道容量的解析解。

4 AWGN 脏纸信道容量

4.1 理想 Costa 算法

在数字水印研究的未热起来之前，Costa[15]提出了下面问题：想象有一页白纸被一些符合正态分布的脏点覆盖，利用有限的墨水在这张纸上写一条消息，然后将这张包含消息的脏纸送给其他人，如果接收者不能区分墨水和脏点，那么能够可靠地传送多少信息？

Costa 把这类问题形象地比喻成一类通信信道，如图 3 所示。这种信道有两个独立高斯白噪声源，信号被传输前就精确地知道第 1 个噪声 s，并将其附加在信号上传输，这个噪声类似于在写信息前白纸上的脏点。传送器传输的信号是功率受限的，即 $\frac{1}{N}\sum_{1}^{N}x[i]^2 < \sigma_w^2$，这类似于用有限的墨水来书写消息。在传输中附加的第 2 个噪声 n 对传送器是未知的，

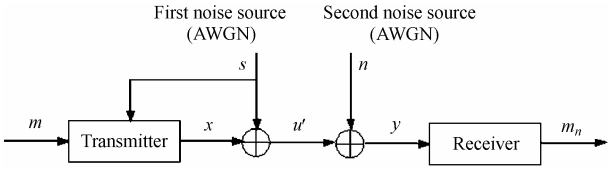

图 3 脏纸信道模型

Fig. 3 Dirty paper channel model

类似于脏纸在传输过程中所遭受的污染。Costa 的脏纸信道模型与具有边信息的盲检测水印系统几乎是完全一致的，脏纸 s 就是载体信号，传输信号 x 就是附加样本，第 2 个噪声源 n 类似于信号处理或恶意攻击所造成的失真。

Costa 定义一类随机码，且这类码中的任一码字都可得到 $I(u;y)-I(u;s)$ 的最大值，从而发现了脏纸信道容量与没有第 1 个噪声源的信道容量相等，显然信道容量不会比这个值再高了，因此这个最大值就是信道容量。Costa 给出了当给定 α 值时的最高可能码率：

$$R(\alpha)=I(u;y)-I(u;s)=\frac{1}{2}\log_2\left(\frac{\sigma_w^2(\sigma_w^2+\sigma_n^2+\sigma_s^2)}{\sigma_w^2\sigma_n^2+\sigma_n^2\sigma_s^2\alpha^2+\sigma_w^2\sigma_s(1-\alpha^2)}\right) \tag{5}$$

Chen和Wornell[16]研究了一种理想的Costa数字水印算法(ICS)，该算法当 $\alpha=\sigma_w^2/\left(\sigma_w^2+\sigma_n^2\right)$ 时，可得 $R(\alpha)$ 的最大值，即 $R(\alpha)=(1/2)\log_2\left(1+\sigma_w^2/\sigma_n^2\right)$。这就是当噪声方差为 σ_n^2 时 AWGN 信道的精确容量，与公式(2)所表示的结果一致。从而得到一个令人惊奇的结果：载体信号对信道容量没有影响。水印设计者们相信：在水印系统中利用边信息，将极大地去除来自载体的干扰。

Costa算法给一般的盲SS水印算法带来了很大希望，但若想得到好的性能，随机码本会很大，实用过程中无论存储还是查找都非常困难。Ettinger提出一种利用结构化码本代替随机码本的标量Costa算法(Scalar Costa Scheme，SCS)[7]，Chen和Wornell[13]以及Su J K 等人[17]也开发了类似的次优Costa算法。

4.2 次优 Costa 算法

SCS 算法的基本原理是假设水印信息 m 被编码成序列 $\boldsymbol{d}=\{d_1,d_2,\cdots,d_N\}$，其中 $d_n=\{0,1\}$。可将 d_n 的嵌入过程看成去抖动量化，如图 4 所示，其中 $\Delta d_n/2$ 是抖动信号，Δ 是均匀标量量化步长。对于 SCS 采用结构化乘积码本 $U^N=U^1\circ U^1\circ\cdots\circ U^1$（$N$ 个 U^1）取代 Costa 算法的随机码本，其中“$\circ$”表示集和直积，$U^1=\left\{u=k\alpha\Delta+d\,\alpha\Delta/2\middle|d\in\{0,1\},k\in Z\right\}$，$\alpha=\sqrt{12\sigma_w^2/\Delta^2}$，并将码本看成是量化器。编码器利用水印信号 W 来干扰原始载体信号 S，从而构成传送信号 $X=S+W$，解码器的作用是量化接收信号 $Y=S+W+N$，这样使 Y 以最大概率落入索引量化器中。

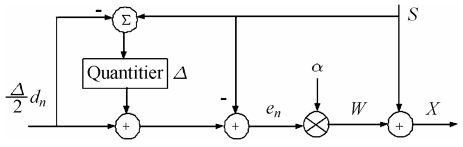

图 4　采用标量码本的 Costa 水印嵌入算法(SCS)

Fig 4 Watermark embedding with Scalar Costa Scheme (SCS)

在 $\sigma_X^2>>\sigma_W^2,\sigma_N^2$ 时，原始载体信号的概率分布可被看成符合均匀分布，标量码本无穷大(由于码本的规则结构是允许的)，在分析中任何边界影响均可被忽略。在假设攻击噪声为高斯白噪声时，则这种算法的信道容量可用式(1)计算得到。

Chen和Wornell[13,18,19]研究了一种叫量化索引调制(QIM)数字水印算法。QIM 是 $\alpha=1$ 时的特殊类型 Costa 传输算法。QIM 可以获得当 WNR 趋于无穷大时的容量。然而，在水印实际应用中 WNR 为负的，且量化单元太小，所以利用 QIM 很难获得可靠的传输。Chen 和 Wornell 又以抖动标量均匀量化为基础提出一种低复杂度 QIM 算法，叫做抖动调制(DM)。这种方法用标量均匀码本模拟 Costa 算法，因为在 Costa 算法中对于每一个 WNR，α 都是获得最好传输性能的最优值。Chen 和 Wornell 用扩展技术改进了在低 WNR 时 DM 算法的鲁棒性，提出了扩展变换的抖动调制(STDM)。这种技术可用于 Costa 算法。

Ramkumar[20]在具有噪声自压缩连续周期函数(CP-SNS)的基础上提出了一种水印算法，其中周期大小与利用结构化码本的Costa算法的单元大小有关。一般情况下两种算法不能互换，然而它们相似的特性对于二进制信号是可以辨识的。在这种情况下，除了量化误差 e_n 加权嵌入被替换成每一个量化误差样本的绝对值最大值限制为 $\beta/2$，具有门限的CP-SNS几乎是和SCS等价的。这样

$$W=\begin{cases}e_n, & |e_n|\le\beta/2\\ \mathrm{sgn}(e_n)\beta/2, & \text{其他}\end{cases}$$

CP-SNS 嵌入过程如图 5 所示。对于 $\beta\ge\Delta$，CP-SNS 和 DM 一样。然而，这里的参数 β 对于每一个 WNR 都可被优化，从而进一步提高了鲁棒性。因此，这个算法的性能总会好于 DM 算法。

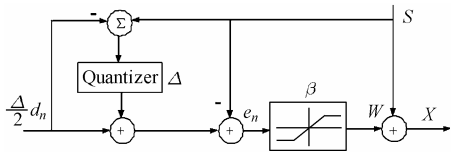

图 5　利用二进制信号样本 CP-SNS 的数字水印嵌入算法

Fig. 5 Watermark embedding using CP-SNS with binary signaling per sample

对于当水印嵌入限制 σ_W^2 一定时，就像在SCS算法中 Δ 和权值 α 的关系一样，量化步长 Δ 和门限 β 是彼此关联的。假设对于概率分布函数基本不变的原始载体信号，在一个量化间隔内，Ramkumar[20]得出如下的关系式：

$$\sigma_W^2=\frac{\beta}{12\Delta}(3\Delta-2\beta)$$

注意，权重为 α 的 SCS 算法可以被看成水印能量最大值 $N\sigma_W^2$ 高维门限。

4.3 容量比较分析

以上介绍的几种基于脏纸模型的数字水印算法—SCS 算法、DM 算法和 CP-SNS 算法的信道容量如图 6 所示。图中的容量曲线是在原始信号为高斯分布情况下获得的，用次优

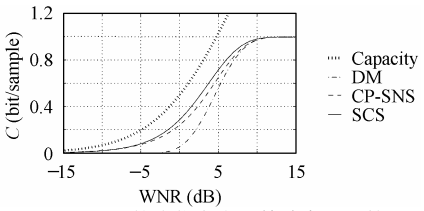

图 6 不同的次优盲水印算法容量比较

Fig6 Capacity compared with the achievable rate of suboptimal blind wate rmarking schemes.

的结构化码本取代无法实现的最优随机码本。结果表明简单的 SCS 算法性能好于其他算法。DM 算法对于负的 WNR 性能较差。因为 SCS 和 CP-SNS 算法都利用优化的 α 和 β 来获得抗噪声的能力，所以 SCS 和 CP-SNS 算法鲁棒性更好。

既然简单的 SCS 算法在几种采用次优的结构化码本的 Costa 算法中鲁棒性最好，那么我们再将其与理想的 Costa 算法和最典型的 SS 算法的容量进行比较。当假设攻击为加性高斯白噪声情况下，采用 SS 算法、ICS 算法和 SCS 算法等的数字水印系统的容量如图 7 所示。从图中可以得出如下结论：原始信号功率仅对 SS 算法有影响(图中显示的是 DWR=15dB 时的信道容量)，盲 SS 受原始信号影响较大；对于弱或中等强度的攻击(例如，WNR> – 10dB)，SCS 算法远远好于 SS 算法，因为 SCS 算法的容量不会因为原始信号的干扰而下降；对于非常强烈的攻击(WNR< – 15dB)，盲 SS 水印容量比 SCS 算法容量大，因为这是攻击失真大于原始信号的影响；然而，对于所有的失真水平 ICS 好于 SS 算法，Costa 证明了利用通信分析水印容量情况下 ICS 算法是最优的，但该算法中的最优随机码本是不可实现的。

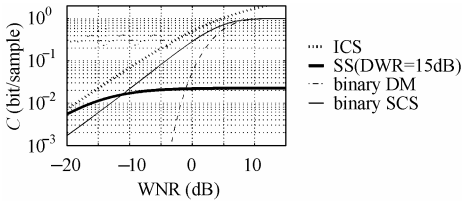

图 7 遭受 AWGN 攻击的各种盲水印算法的容量

Fig7 Capacity of blind watermarkings facing different AWGN attack

5 基于游戏理论分析信道容量

与用传统的信息论分析水印容量方法不同，Moulin和O'Sullivan等人[7,21,22]将水印看成是信息隐藏者与敌手间的游戏，信息隐藏者嵌入水印到载体对象中，而敌手企图去除这些水印，所以他们结合游戏理论来分析带边信息的水印系统的信道容量。

5.1 作为游戏的水印[5,6]

水印的游戏理论主要是建立在失真函数、水印代码和攻击信道这样 3 个概念的基础，它们的定义如下：

(1) 失真函数 是一个实函数用 $D(C_1,C_2)$ 表示，其中 C_1 指原始载体信号，C_2 是 C_1 的失真版本，$D(C_1,C_2)$ 随着两个信号间的差别而单调变化。一般情况，Moulin 和 O'Sullivan 假设 $D(C_1,C_2)$ 只是应用于 C_1 和 C_2 某个失真函数的一个标准扩展，即

$$D(C_1,C_2)=\frac{1}{N}\sum_{i}^{N}d(c_1[i],c_2[i]) \tag{6}$$

(2) 水印代码 是满足失真为 D_1、长度为 N 的信息隐藏代码。它包括 3 个部分：(a) 消息集 M；(b) 水印嵌入函数 $\mathcal{E}_K(C_0,m)$，其中 C_0 是维数为 N 的未加水印信号，$m\in M$ 是消息，且 K 是水印密钥；(c) 水印检测函数 $D_K(C)$，其中 C 是加水印信号(也可能是未加水印信号)，K 是密钥。

要求嵌入过程限制水印嵌入函数，使其产生的期望失真小于或等于失真 D_1，即

$$\sum_{C_o,K,m}\frac{1}{|M|}P_{c_oK}(C_o,K)D(C_o,\mathcal{E}_K(C_o,m))\le D_1 \tag{7}$$

此式是针对于原始载体信号 C_0，密钥 K 及消息 m 的所有可能组合来求和的。$P_{C_0,K}(C_0,K)$ 是应用密钥 K 于 C_0 的联合概率分布，用于处理当密钥依赖于原始载体信号的情况。

(3) 攻击信道 为满足失真 D_2 的攻击信道 $Q_2(C_n/C)=P_{C_n}(C_n)$，是一个条件概率函数，表明对加水印信号 C 应用某特定的攻击后获得 C_n 的概率。当对加水印信号应用攻击后，限制这个概率函数，以便产生的期望失真小于或等于 D_2。即

$$\sum_{C_n,C}P_C(C)Q_2(C_n/C)D(C,C_n)\le D_2 \tag{8}$$

式中 $P_C(C)$ 是在随机选择的原始载体信号中嵌入随机信息后获得 C 的概率，即嵌入失真。

在失真为 (D_1,D_2) 的信息隐藏游戏中，信息隐藏者设计一种失真为 D_1 的信息隐藏代码，而敌手设计一种失真为 D_2 的攻击信息。信息隐藏者企图使信道传输的信息最大化，而敌手欲使其最小化。如果可以设计一种具有最小速率 R 的信息隐藏代码，以使经过最坏的攻击后，当 N 增至无穷大时，错误概率减小为 0，那么在失真 (D_1,D_2) 下可获得给定速度 R。数据隐藏容量 $C(D_1,D_2)$ 是对于失真 (D_1,D_2) 所有可获得速率上限。

5.2 信道容量的一般表示式

Moulin 和 O'Sullivan 的主要研究成果是给出了数据隐藏容量 $C(D_1,D_2)$ 的一般性表达式，像 Gelfand 和 Pinsker 带边信息的通信容量的表达式一样，这个表示式也利用辅助变量 U。

他们认为水印的嵌入算法可被分成两步：第 1 步是根据期望的消息 m，载体信号 C_0 和密钥 K 来寻找 U 值。假设消息服从均匀分布，这样根据未加水印内容和密钥分布可得 U 的条件分布 $P_{U/c_0,K}(U)$。第 2 步，根据值 U 和未加水印信号 C_0，参考密钥 K 可获得加水印的信号 C。那么从给定的原始载体信号、密钥可得到加水印信号的分布：

$$Q_1(C,U\mid C_0,K)=P_{C|c_0,U,K}(C)P_{U|C_0,K}(U) \tag{9}$$

一般说来，在满足嵌入失真的限制的条件，可以设计一种嵌入算法对于 $Q_1(\,)$ 可得到任何要求的分布：

$$\sum_{C,C_0,U,K}D(C,C_0)Q_1(C,U\mid C_0,K)P_{C_0,K}(C_0,K)\le D \tag{10}$$

对于失真 (D_1,D_2) 数据隐藏游戏的容量为

$$C(D_1,D_2)=\max_{Q_1}\min_{Q_2}\left[I(U;C_n/K)-I(U;C/K)\right] \tag{11}$$

式中最大化是针对满足于失真限制 D_1 的所有嵌入水印后信号分布，而最小化是针对所有满足失真限制 D_2 的攻击信道。$I(U;C/K)$ 是 U 和 C 间的互信息，其二者的概率分布是在条件 K 下计算。

如果承认 $I(U;C_n/k)-I(U;C/k)$ 的最大最小值本质上与 Gelfand 和 Pinsker 的表达式(式(4))中的最大值一样，则式(11)直观上容易理解。这样如果限制可能的攻击后信号分布为一种特定的分布，那么可以获得在传送器端具有边信息的通信容量。

当然，敌手不会限于仅使用一种攻击，他们会选择一种使通信的信息总量最小的一种攻击。所以对于给定分布 Q_1，可以传输信息总量是所有可能攻击中的最小值，最好的 Q_1 (从数据隐藏者的角度考虑)是这些最小值中的最大值。这样数据隐藏容量是所有可能 Q_1 的最大值，和所有可能 Q_2 的最小值。

式(11)的值依赖于 D_1, D_2 和失真函数 $D(C_1,C_2)$，它可能依赖于/或可能不依赖于未加水印信号的分布。对于给定的信号类型，存在最好地反映人的知觉特性的单一失真函数，和未加水印信号的单一分布。这样，从理论上讲，数据隐藏上的容量决定于 D_1, D_2 和载体信号类型。然而对于图像，视频和音频，最好的失真函数和真实的失真函数不知道，因此式(11)只能用于在一些简化的假设下来获得容量的估计值。

5.3 均方误差(Mean Square Error, MSE)保真度限制的容量

Moulin 和 O′Sullivan 对隐藏容量的分析基于以下两个假设：

(1) $D(C_1,C_2)$ 是均方误差(MSE)，即 $D(C_1,C_2)=\frac{1}{N}\sum_i^N(c_2[i]-c_1[i])^2$。

(2) 载体 C_0 是服从方差 $\sigma_{c_0}^2$ 的独立同分布(IID)的高斯分布。

那么隐藏容量 $C(D_1,D_2)$ 为

$$C(D_1,D_2)=\begin{cases}0, & D_2\ge\sigma_{c_0}^2+D_1\\ \frac{1}{2}\log_2\left[1+D_1/(\beta D_2)\right], & \text{其他}\end{cases} \tag{12}$$

式中 $\beta=\left(1-D_2/\left(\sigma_{c_0}^2+D_1\right)\right)^{-1}$。

从上式中可以看出，当 $D_2\ge\sigma_{c_0}^2+D_1$，则敌手可简单地使加水印信号为 0 来去除水印。很明显，经过这样的攻击后，信息无法保留住，容量为 0。当 $D_2<\sigma_{c_0}^2+D_1$，最优攻击将是高斯测试信道生成等价的 AWGN 脏纸信道，无论检测器是盲的，还是含辅助信息的，容量都是 $\frac{1}{2}\log_2\left[1+D_1/(\beta D_2)\right]$。

与 Costa 的脏纸信道容量不同，在 β 依赖于 $\sigma_{c_0}^2$ 的数据隐藏的游戏中，未加水印信号的分布影响容量，原因在于它影响敌手所采取攻击的严重性。在 $D(C_1,C_2)$ 为 MSE 失真函数条件下，较小的 $\sigma_{c_0}^2$ 值允许敌手采用更严重的失真。在第 1 步中加入更多噪声，在第 2 步中利用大的 β 缩小结果向量，使其在可接受保真度区域内。而对于更实际的考虑到掩蔽效应的失真函数，$\sigma_{c_0}^2$ 越大，就允许失真越严重，因为它们暗示每个信号可容纳更多噪声，这样有较强的隐藏失真能力。故在每一种情况下，都存在 $\sigma_{c_0}^2$ 影响容量这一定性特点。从式(12)可得出的第 2 个定性结论是：当 $D_1,D_2\ll\sigma_{c_0}^2$ 时，$\sigma_{c_0}^2$ 对容量的影响较小。当 $D_2/\sigma_{c_0}^2$ 趋于 0 时，β 趋于 1，容量趋于 $(1/2)\log_2(1+D_1/D_2)$。因为一般假设 D_1 和 D_2 相对于 $\sigma_{c_0}^2$ 较小，因此，也就意味着水印和攻击都是不可见的，所以 $\sigma_{c_0}^2$ 可被忽略。此外还可得出第 3 个定性结论：当 $D_1,D_2\ll\sigma_{c_0}^2$ 时，未加水印信号分布的形状可以不考虑。

6　结束语

本文总结了利用信息论和游戏理论分析数字水印信道容量的研究结果。经典的非盲扩频水印算法和理想的 Costa 算法，理论上可以达到最大水印容量，因为它们都可以去除水印载体信息的影响。但非盲的扩频水印算法检测时需要原始的载体信息，在实际应用时受到限制；理想的 Costa 算法，要达到最大的理论容量，必须建立随机码本，而理想的随机码本的建立和搜索都是无法实现的。所以，这两种算法只能为我们设计实际可实现的算法提供理论指导。从对基本通信模型的信道容量、边信息水印模型的信道容量及基于游戏理论的信道容量的分析可以看出，数字水印系统的信道容量与水印噪声比(WNR)密切相关，总体趋势是随着 WNR 的增大，水印信道容量也单调增大。对于将载体对象看作是水印嵌入器的辅助信息的水印系统，利用边信息的通信模型来分析，总的来说这种系统的容量好于基本水印模型的容量，水印编码考虑到原始载体信号，利用量化实现结构化的次优编码。通过对安全水印的分析可知，最佳的攻击策略是一种特殊的率失真问题的解，最佳的嵌入策略是一个信道编码问题，所以我们可以从率失真及信道编码的角度去研究有效的水印算法。

参 考 文 献

[1] Cox I J, Miller M L, Bloom J M. Digital Watermarking. United States of America, Mordan Kaufmann Publishers, 2002, chapter 1 − 2.

[2] Perez-Gonzalea F, Hernandes J R, Balado F. Approaching the capacity limit in image watermarking: a perspective on coding techniques for data hiding applications. *Signal Processing* 2001, 81(6): 1215 − 1238.

[3] Su J K, Eggers J J, Girod B. Capacity of digital watermarks subjected to an optimal collusion attack. European Signal Processing Conference(EUSIPCO), Tampere, Finland, September 2000.

[4] Eggers J J, Bauml R R, Girod B. Digital watermarking facing

attacks by amplitude scaling and additive white noise. 4th Intl. ITG Conference on Source and Channel Coding, Berlin, Jan. 2002: 28－30.

[5] Moulin P, O'Sullivan J A. Information-Theoretic Analysis of Information Hiding. *IEEE Trans. on Information Theory*, 2003, 49(3): 563－593.

[6] Moulin P, O'Sullivan J A. Information-theoretic analysis of watermarking. in Proceedings of the International Conference on Acoustics, Speech, and Signal processing, 2000, 6: 3630－3633.

[7] O'Sullivan J A, Moulin P, Ettinger J M. Information-theoretic analysis of steganography. Proceedings of the IEEE International Symposium on Information Theory, Boston, Aug. 1998.

[8] Eggers J J, Bauml R, Girod B. A communications approach to image steganography. Proceedings of SPIE Vol.4675, Security and Watermarking of Multimedia Contents IV, San Jose, Ca., Jan., 2002.

[9] Cachin C. An information-theoretic model for steganography. Information Hiding, 2nd International Workshop, volume 1525 of Lecture Notes in Computer Science, Springer, 1998: 306－318.

[10] 傅祖芸. 信息论—基础理论及应用. 北京: 电子工业出版社，2001: 90－111.

[11] Cox I J, Kilian J, Leightom T, Shamoon T. Secure spread spectrum watermarking for multimedia. *IEEE Trans. on Image Processing*, 1997, 6(12): 1673－1687.

[12] Cox I J, Miller M L, McKellips A. Watermarking as communications with side information. *Proceedings of the IEEE*, 1999, 87(7): 1127－1141.

[13] Chen B, Wornell G W. Achievable performance of digital watermarking systems. In Proceeding of the IEEE Intl. Conference on Multimedia Computing and Systems (ICMCS'99), Florence, Italy, July 1999, 1: 13－18.

[14] Gelfand S I, Pinsker M S. Coding for channel with random Parameters. *Problems of Control and Information Theory*, 1980, 9(1): 19－31.

[15] Costa M. Writing on dirty paper. *IEEE Trans. on Information Theory*, 1983, 29(3): 439－441.

[16] Chen B, Wornell G W. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Trans. on Information Theory*, 2001, 47(4): 1423－1443

[17] Su J K, Eggers J J, Girod B. Andysis of digital watermarks subjected to optimum linear filtering and additive noise. *Signal Processing*, 2001, 81(6): 1141－1175.

[18] Chen B, Wornell G W. Dither modulation: a new approach to digital watermarking and information embedding. In Proceeding of SPIE Vol. 3675. Security and Watermarking of Multimedia Contents, San Jose, January 1999.

[19] Chen B, Wornell G. Proprocessed and postprocessed quantization index modulation methods for digital watermarking. In Proceeding of SPIE Vol.3971; Security and Watermarking of Multimedia Contents Ⅱ, San Jose, January 2000.

[20] Ramkumar M. Data hiding in multimedia: theory and application. Ph. D thesis, New Jersey Institute of Technology, Kearny, NJ, USA, 1999.

[21] Moulin P, Mihgak M K. The parallel-gaussian watermarking game. UIUC Technique Report UIUC-ENG-01－2214, June 2001.

[22] Moulin P, Ivanovic A. The watermark selection game. Proceeding Conference on Information Sciences and Systems, Baltimore, MD, March 2001.

王 颖： 女，1969年生，副教授，研究方向为数字通信、数字图像处理、数字水印技术.

李象霖： 男，1938年生，教授，研究方向为数字图像处理、数字水印技术.