基于信息论的数字水印研究

张向华 韦鹏程
(重庆教育学院计算机与现代教育技术系 重庆 400067)

摘 要 提出一种运用通信系统理论研究数字水印系统的方法。通过分析水印信道的特性来研究水印系统的性能，通过计算有关信号的交互信息、条件熵等数据对水印系统的嵌入强度、嵌入位置等问题进行了分析，推导出有效提取水印的信息论下限的方法，所得结果对于设计水印算法具有较强的指导作用。

关键词 信息论，数字水印，信道容量，交互信息

Study of Digital Watermarking Based on Information Theory

ZHANG Xiang-hua WEI Peng-cheng
(Dept. of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067, China)

Abstract A method of studying watermarking system using the theory of communication was presented. An information theoretic analysis of the intensity and position embedding and the capacity of watermarking channel, as well as an information theoretic bottom bounds for extraction effectually of watermark was proposed through calculating the mutual information and conditional entropy of the correlated signals. The results have a good role in guiding the designing of watermarking system.

Keywords Information theory, Digital watermarking, Channel capacity, Mutual information

1 引言

对于水印系统，我们可以把载体图像视为加在水印信号上的强噪声扰动，将其作为一个通信问题[1]，通过分析水印信道的特性来研究水印系统的性能，从而可以用 Shannon 信息论的观点来研究水印技术的一些基本问题。J. Cox[2] 和 P. Moulin [3] 分别建立了信息隐藏和数字水印的信道模型，并运用限失真编码理论比较详细、深入地研究了信道的容量问题，推导出达到最大信道容量的条件。Costa[5] 证明了“在水印检测时，不论是否知道载体图像(即是否采用盲水印)，水印信道的容量相同”的惊人结论。他们的研究结果对于设计水印算法很有指导意义，对我们的研究也有启示。从已有的研究结果来看，一个有效的数字水印系统应具备两个最基本的特性：①不可感知性。即嵌入水印的图像和原始图像对人的感觉器官应该是没有差别的；②鲁棒性。给定一个含水印的图像，经过图像处理(如 JPEG 压缩、低通滤波、加噪、剪切等)后，仍然能提取出有效的水印信息。由于这是两个互相制约、相互矛盾的因素，对于一个水印算法而言，必须要折衷考虑。这实质上是一个如何确定水印的嵌入能量问题[4]。嵌入多强的水印信号能够达到既有好的透明性又有好的鲁棒性，是一个需要深入研究的问题，也是数字水印算法的关键之一。本文运用 Shannon 信息论，通过分析水印信道的特性来研究水印系统的性能，从理论上对水印算法设计中所涉及到的嵌入强度、嵌入位置和水印信道的容量等问题进行了研究，推导出相应的计算公式。

2 数学模型

一个数字水印系统，可以看作是带有附加信息的通信系统。以图像水印为例，从目前已有的水印算法来看，可以将其近似为信源功率 P_m 受限，信源 M、载体 S、噪声 N 都是高斯分布的高斯加性信道，且 M 与 S 之间、S 与 N 之间统计独立，$(MS)XY$ 构成马尔可夫链，如图 1 所示。

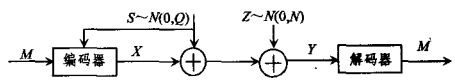


图 1 数字水印高斯信道

图 1 所示的水印信道，M 为信源，即水印系统中需嵌入的水印；$S\sim N[0,Q]$ 为加在信道上的强噪声，即水印系统中的载体；$X\sim N[0,P]$ 为经过编码后的混合信号，为信道的输入，即水印系统中嵌入水印后的载体；$Z\sim N[0,N]$ 为信道噪声，即水印系统中对水印载体所采取的有损压缩、滤波、尺寸变换、重采样等处理。对水印系统有两个基本要求：鲁棒性和不可感知性，利用图 1 所示的模型，运用信息论的观点，可以用交互信息来刻画这两个要求。

①不可感知性：相当于要求载体 S 与水印载体 X 之间的

到稿日期：2008-07-01 本文受重庆市科委自然科学基金计划资助项目(CSTC, 2006BB2254)，重庆市教委资助项目(KJ071504, No. kj061501)资助。

张向华(1969－)，男，副教授，硕士，主要研究方向为混沌理论及其信息安全；韦鹏程(1975－)，男，副教授，博士，主要研究方向为混沌理论及其信息安全。

交互信息 $I(S;X)$ 要尽可能大，同时希望水印 M 与水印载体 X 之间的交互信息尽可能小。若 $I(M;X)=0$，即 M 与 X 之间完全不相关，用信息隐藏的术语讲，称为完善隐秘系统。

②鲁棒性：就是要求信道的输出 Y 与嵌入的水印 M 之间的交互信息 $I(M;Y)$ 在允许的信道上尽可能大。由于要可靠地判定 Y 中是否包含水印，至少需要一位的信息，因此 $I(M;Y)\geqslant 1$。而要完全恢复水印 M，则至少需要 $I(M)$ 位。

当然，有关水印的不可感知性、鲁棒性及其他特性，还可以用不同的信息论语言来描述。

3 数字水印算法分析

3.1 水印信道的信道容量

参考图 1 的信道，对于离散无记忆信道，当编码器确知状态 S 时，其信道的容量为

$$C=\max_{p(u,x|s)}\{I(U;Y)-I(U;S)\} \tag{1}$$

其中，$U=X+\beta S$，为一有限符号集的辅助随机变量，X 和 S 分别是分布为 $N(0,\sigma_x^2=P)$ 和 $N(0,\sigma_s^2=Q)$ 的独立随机变量，β 为待定参数，$X=M\oplus S$ 且 $(1/n)\sum_{i=1}^{n}x_i\leqslant P$。式中的最大要取遍 $p(s)p(u,x|s)p(y|x,s)$ 的所有联合分布。输出 $Y=X+S+Z$，$Z\sim N(0,\sigma_z^2=N)$。

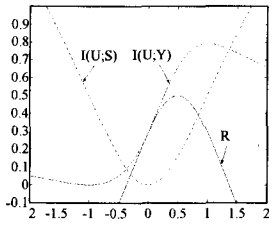
对图 1 所示水印信道，其信息传递速率 R 为[3]：

$$R(\beta)=\frac{1}{2}\log_2\left(\frac{P(P+Q+N)}{PQ(1-\beta)^2+N(P+\beta^2Q)}\right) \tag{2}$$

因此，其信道容量 C 为

$$C=\max_{\beta}R(\beta)=\frac{1}{2}\log_2\left(1+\frac{P}{N}\right) \tag{3}$$

为较直观地表现 $R(\beta)$，$I(U;Y)$，$I(U;S)$ 与 β 间的关系，取 $P=Q=N=1$，$\beta\in[-2,2]$ 时的函数值随 β 变化的曲线做图，如图 2 所示。



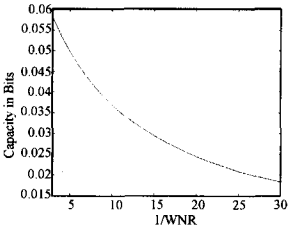


图 2 $I(U;Y)$，$I(U;S)$，$R(\beta)$ 曲线　　图 3 信道容量变化曲线

3.2 有效提取水印的信噪比下界

根据 Shannon 理论，信道传输速率 R 与信源所发出的符号数有直接关系：

$$R=\frac{\log M}{N}\quad \text{比特/码符号} \tag{4}$$

其中，M 为信源输出的消息数，N 为随机编码的码字长度，R 为当信道的 M 个输入消息先验等概时信道编码的每一个码符号所携带的平均信息量，即码率。按照 Shannon 第二定理，需要传递的等概消息数 M 只要不超过 $2^{N(C-\varepsilon)}$，平均差错译码概率可无限接近于零。当所需传递的消息数 $M\to 2^{N(C-\varepsilon)}$ 时，信道的信息传输率(码率)：

$$R=\frac{\log M}{N}\to\frac{N(C-\varepsilon)}{N}=C-\varepsilon \tag{5}$$

其中 ε 是任意小的正数，所以这时的信道信息传输率 R 可以无限接近信道容量 C。

从式(3)可知，水印信道容量是水印信号与系统所受到噪声的比值的函数。水印系统中噪声由相互独立的两部分组成：一部分是载体图像的强噪声；另一部分是混合图像所受到的攻击噪声，即 $\sigma_n^2=\sigma_s^2+\sigma_p^2$。当 $\sigma_p^2=0$ 时，将式(3)简化为

$$C^*=\frac{1}{2}\log_2(1+WNR) \tag{6}$$

其中，WNR 为不计处理噪声时水印信号能量与噪声能量的比值(dB)。将式(6)做图，如图 3 所示。从图中可以看出，WNR 的值越小，信道的容量越小，所能传输的数据量也就越小，导致所能嵌入的数据就少。当水印系统一定后，所需经过信道传输的最大符号数 M 是一定的。为确保接收端能收到正确提取(或检测)所需的信息量，必须有

$$C\geqslant M \tag{7}$$

成立，于是可得：

$$WNR\geqslant 10\log_{10}(M_N^2 2^{2\alpha}-1) \tag{8}$$

其中 ε 为任意小的正数。这就是我们希望得到的结论。当一个水印系统确定之后，M，N 便是确定的值，由式(8)就可以计算出确保能提取(检测)出有效水印所必需的信噪比分析(WNR)下限。

3.3 水印嵌入强度(强度因子 α)

作为通信问题的水印系统，载体图像 S 为加在待传输的信息 M(水印)上的强噪声，设嵌入水印后的混合图像为 X，若嵌入算法为 $X=S+\alpha M$，则由信息论中信噪比的定义：

$$WNR=10\lg\left(\frac{\sum\sum(X_k^2-S_k^2)}{\sum S_k^2}\right)=10\lg\left(\frac{\alpha^2\sum M_k^2}{\sum S_k^2}\right) \tag{9}$$

可以得到

$$\alpha=\sqrt{\frac{\sum S_k^2}{\sum M_k^2}10^{\frac{WNR}{10}}} \tag{10}$$

式(10)给出了水印算法设计中经常要用到的确定嵌入强度的理论依据。其实，此式给出的是一个强度因子的下限值。我们通过对 Lena，Pepers，Banboo 等标准图像进行实验，发现即使是在这些图像的低频系数上，按照式(10)计算的强度嵌入，混合图像仍然有很好的透明性。如果结合人类视觉模型，就可以摆脱只凭经验和实验确定嵌入因子的局限。

3.4 水印嵌入位置分析

从式(3)可知，$\sigma_n^2=\frac{\sigma_m^2}{2^{2c}-1}$。当容量 C 为确定值时，水印信号能量与噪声能量成正比。即水印信号的能量越大，所能抵抗的噪声能量也越大，则水印系统鲁棒性越强。而 $\sigma_n^2=\sigma_s^2+\sigma_p^2$，从鲁棒性考虑，$\sigma_p^2$ 要尽量大，在信道容量一定的情况下，所能经受的 σ_n^2 是有限的，则只有尽量减小 σ_s^2 的数量。但是，载体图像确定后，σ_s^2 是不变的，于是我们可考虑：

①水印算法确定后，所能经受的干扰是有限的，则其所能抵抗的攻击能量 σ_p^2 也是有限的。当攻击能量大于 σ_p^2 时，就不能确保水印能有效提取，或者说提取出的水印与原始水印的相似度很低。

②可以通过寻求一种嵌入算法 $X(S,M)$，使 X 中的 σ_s^2 含量较低。这有两种考虑：一是限制高能量分量，即通过一种水印嵌入方法，使最高的成分降下来；另一种就是将水印嵌入到低能量分量中，使较低的成分升上去，即将水印信号嵌入到 S 的能量较高或较低的部分，并可分别采用相减和相加的嵌入公式，以减小 σ_s^2 数值。

4 讨论

4.1 对非高斯分布时的处理

在式(2)和式(3)中要求 Y 具有高斯分布时才能达到信

(下转第 255 页)

```
}
    glEnd();
    glDisable(GL_TEXTURE_2D);
    glDisable(GL_ALPHA);
    glDisable(GL_BLEND);
GLdouble eqn[4] = {a,b,c,d};
    glClipPlane (GL_CLIP_PLANE0,eqn);
    glEnable (GL_CLIP_PLANE0);
    绘制器官表面模型;
    glDisable(GL_CLIP_PLANE0);
```

4 实验结果与分析

通过读取经缩小比例后的数字化猪1157张RGB断面切片，925张躯干序列轮廓(位于原始切片1～1850间)及大部分躯干面绘制模型(位于原始切片484～1844间)，进行躯干内部器官的任意剖切显示。操作者可以通过切平面控制面板控制切平面的方向和位置，实现对数字化猪躯干部分的任意切割和连续切割，其中任意切割采用高精度的立方体三线性插值抽取剖切面纹理保证显示效果，对任意方向连续切割的实时动画采用速度较快，精度略低的立方体邻近插值抽取切面纹理，从而在显示的速度和精度上达到平衡。图2给出了采用本文方法剖切的数字化猪躯干部分。

图2 数字化猪躯干任意切割剖切面效果图

结束语 本文为基于图像序列轮廓三维重建表面的任意切面纹理提取及映射提供了一个简单有效的方法，其创新点为：(1)通过将纹理贴在切平面多边形上而不是直接贴在形状复杂的模型剖切面上，避免了模型剖切面的多边形链化、三角化、纹理映射等大量运算；(2)剖切面纹理提取时，用矢量叠加原理确定纹理图像中每个像素在图像序列空间中的位置，避免将每个像素都和变换矩阵相乘，从而较大幅度地提高了运行速度。实践证明该方法能准确、快速地对数字化猪器官进行任意剖切面的纹理显示。

参考文献

[1] 潘群娜，熊小飞. 基于人脑部体数据的任意切面研究[J]. 微计算机信息：测控自动化，2007，23(7-1)：269-273

[2] 徐鹏，尧德中. 一种在三个医学剖面上任意切面图像提取的有效方法[J]. 计算机应用，2005，25(2)：320-325

[3] 张艳君，叶伯生，曾理湛. 基于医学图像序列轮廓线重建三维表面的改进算法[J]. 计算机工程与应用，2004，13：215-218

[4] 陈传波，陆枫. 计算机图形学基础[M]. 北京：电子工业出版社，2005：125-127

[5] Shreiner D，Woo M，Neider J，et al. OpenGL 权威编程指南(原书第五版)[M]. 徐波，等译. 北京：机械工业出版社，2006

(上接第249页)

道容量C。信息论指出，当输入信源X为高斯分布时，才能使Y成为一个高斯分布的随机变量。当载体图像被分解后，其统计分布有可能不是高斯分布，此时需要对其进行高斯化处理，以获得高斯分布的σ_{ig}^2。为计算σ_{ig}^2，我们做如下变换：

①计算载体图像的方差σ_{ij}^2(若采用了DCT或DWT分解，则计算出各个系数的σ_{ij}^2)，把具有相近σ_{ij}^2值的系数点视为一个通道；

②画出各个通道的直方图，并计算其信息熵。设Δx为区间n的宽度，$g(m)$，$m=1,2,\cdots,n$为频数累计值，p为各个频道中系数总数，信息熵和伪高斯分布方差σ_{ig}^2为：

$$H_j=-\sum_{i=1}^{n}\frac{g(i)}{p\Delta x}\log_2\left(\frac{g(i)}{p\Delta x}\right)\Delta x,\sigma_{ig_j}^2=\frac{2^{2H_j}}{2\pi e}$$

③频域水印技术将载体图像分解成多个频段后再嵌入水印。根据通信理论，可将其视为多通道的独立并列信道。设载体图像被分解成L个通道，每个频道都有相应的两个噪声，其信道容量为[9]

$$C=\frac{XY}{2L}\sum_{j=1}^{L}\log_2\left(1+\frac{\sigma_{mj}^2}{\sigma_{igj}^2+\sigma_{pj}^2}\right) \tag{11}$$

其中，XY为图像的像素，σ_{ig}^2为伪高斯分布的图像方差。

4.2 载体能量对鲁棒性的影响

我们从式(3)还可看出，在保持最大容量C不变的情况下，水印载体能量P越大，所能经受的噪声干扰能量N也越大，即水印的鲁棒性越强；水印载体所受噪声干扰越小，所能嵌入的水印信息量越大，水印的鲁棒性也就越好。

4.3 其他方法

水印信道的容量可以根据编码者、解码者、攻击者的不同目的有不同的表示方法[3]。同时，信息论中的编码理论，特别是限失真信源编码，也是分析水印算法的有力工具。这些内容及问题我们将在今后的研究中进行深入的探讨。

结束语 本文提出一种运用通信系统理论研究数字水印系统的方法。通过分析水印信道的特性来研究水印系统的性能，通过计算有关信号的交互信息、条件熵等数据对水印系统的嵌入强度、嵌入位置等问题进行了分析，推导出有效提取水印的信息论下限，所得结果对于设计水印算法具有较强的指导作用。

参考文献

[1] 刘瑞祯，谭铁牛. 数字图像水印研究综述. 通信学报，2000，21(8)：8-14

[2] Cox J，et al. Watermarking as Communications with Side Information//Proceeding of the IEEE. 1999，87(7)：1127-1141

[3] Moulin P. Information-Theoretic Analysis of Information Hiding. IEEE Trans on Information Theory，2003，49(3)：563-593

[4] Cohen A S，et al. The Gaussian Watermarking Game. IEEE Trans on information theory，2002，48(6)：1639-1667

[5] Costa M M. Writing on Dirty Paper. IEEE Trans on information theory，1983，29(5)：439-441

[6] 刘瑞祯，谭铁牛. 水印能量估计的一般性框架. 计算机学报，2001，24(3)：242-246

[7] 姜丹. 信息论与编码. 合肥：中国科学技术大学出版社，2001