



数字水印的定义



数字水印的定义

数字水印是永久镶嵌在其他数据（宿主数据）中具有可鉴别性的数字信号或模式，并且不影响宿主数据的可用性。



数字水印的特点

安全性

数字水印难以被发现、擦除、篡改或伪造，同时，要有较低的虚警率

可证明性

数字水印应能为宿主数据的产品归属问题提供完全和可靠的证据

不可感知性

从感观上和统计上都不可感知

稳健性

数字水印应该难以被擦除，任何试图完全破坏水印的努力将对载体的质量产生严重破坏

好的水印算法应该对信号处理、几何变形、恶意攻击等具有稳健性



衡量水印算法稳健性的处理 (1)

数据压缩处理

图像、声音、视频等信号的压缩算法是去掉这些信号中的冗余信息。通常，水印的不可感知性就是采用将水印信息嵌入在载体对感知不敏感的部位，而这些不敏感的部位经常是被压缩算法所去掉的部分。

滤波、平滑处理

水印应该具有低通特性，低通滤波和平滑处理应该无法删除水印。



衡量水印算法稳健性的处理 (2)

量化与增强

水印应该能够抵抗对载体信号的A/D转换、D/A转换、重采样等处理，还有一些常规的图像操作，如图像在不同灰度级上的量化、亮度与对比度的变化、图像增强等，都不应该对水印产生严重的影响。

几何失真

几何失真包括图像尺寸大小变化、图像旋转、裁剪、删除或添加等。



数字水印三要素

水印本身的结构

- 版权所有者、合法使用者、日期等具体信息
- 伪随机序列

水印的加载过程

水印的检测过程



数字水印加载和检测流程





水印的加载

设 I 为数字图象, W 为水印信号, K 为密钥, 处理后的水印 \tilde{W} 由函数 F 定义如下

$$\tilde{W} = F(I, W, K)$$

水印嵌入过程

设有编码函数 E , 原始图象 I 和水印 \tilde{W} , 嵌入水印后的图象为

$$I_W = E(I, \tilde{W})$$



水印的检测

水印检测过程

设解码函数为 D ，水印提取的两种形式：

- 提取原始水印：如文字、徽标
- 0-1判决：判定水印存在与否

$$W^* = D(\hat{I}_W, I, K)$$

$$C(W, W^*, K, \delta) = \begin{cases} 1, & W \text{ 存在} \\ 0, & W \text{ 不存在} \end{cases}$$



可能的两类错误

- ✓ 第一类错误: 实际不存在水印但却检测到水印, 该类错误用虚警率(误识率) P_{fa} 衡量。
- ✓ 第二类错误: 实际有水印但是却没有检测出水印, 用漏检率 P_{rej} 表示。

总错误率为 $P_{err} = P_{fa} + P_{rej}$