DOI:10.16208/j.issn1000-7024.2005.03.019



# 数字水印的鲁棒性分析与研究

袁占亭， 张秋余， 陈 宁
(兰州理工大学 电气工程与信息工程学院，甘肃 兰州 730050)

**摘 要**：讨论了数字图像水印系统的基本框架，简要介绍了系统各个组成部分所完成的功能。详细阐述了数字水印鲁棒性的概念、影响鲁棒性的因素、实现鲁棒性的策略以及鲁棒性评估的描述方法，并说明了鲁棒性在水印系统中的重要地位。最后基于盲检测器水印模型提出了一种估计水印鲁棒性的算法，并给出了算法的描述。由于该算法与扩频技术具有相同的理论依据并且计算过程比较简单，因此在理论上是合理有效的。

**关键词**：鲁棒性； 保真度； 抗攻击力； 盲检测器； 数字水印
**中图法分类号**：TP309; TP391 **文献标识码**：A **文章编号**：1000-7024 (2005) 03-0614-03

# Analysis and study of robustness of digital watermarking

YUAN Zhan-ting, ZHANG Qiu-yu, CHEN Ning
(College of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou 730050, China)

**Abstract**: The basic frame of digital image watermarking system is discussed, and the functions of every part in the watermarking system is introduced briefly. The concept of the robustness, the factors affecting the robustness, the strategies used to realize the robustness and the methods evaluating the robustness are set forth at length and the importance of robustness in digital watermarking system is explained. Finally, an arithmetic used to estimate the robustness of digital image watermarking system is put forward, which is based on the watermarking model with blind detector. And the description of the arithmetic is given. Because this arithmetic has the same academic gist with spread-spectrum technique and has easy computing process, it is reasonable and effective theoretically.

**Key words**: robustness; fidelity; anti-attack ability; blind tester; digital watermarking

## 1 引 言

随着计算机多媒体技术和因特网技术的迅猛发展，人们可以很方便地传播、拷贝、存储和处理图像、音频和视频等多媒体信息。与此同时，也引发了各种多媒体信息的传输安全问题和数字产品的版权保护问题。为了更好的解决数字内容的版权保护和信息安全问题，人们提出了“数字水印”的概念。与其他技术相比，数字水印技术有其自身的优势，它可以弥补加密技术、数字签名技术、数字标签以及数字指纹等技术的缺陷和不足。为此，它成为当前多媒体信息安全研究领域发展最快的热点技术，已经受到国际学术界和企业界的高度关注。为了支持数字水印技术在各个领域中的应用，我们有必要对其性质，尤其是鲁棒性做进一步的分析和研究，因为它直接关系到各种水印应用的可靠性和稳定性。

## 2 数字水印的基本框架

### 2.1 通用水印框架

下面以数字图像水印为例说明水印的通用框架(GWF)[1]，它可用六元组$(X,W,K,G,\xi,D)$表示，其中：

(1) X 表示要被保护的数字产品$\tilde{X}$的集合；

(2) W 是水印信号集合；

(3) K 是水印密钥空间；

(4) G 表示用某密钥与要加水印的数字产品产生水印的水印生成算法

$G:X\times K\to W \quad \tilde{W}=G(\tilde{X},\tilde{K})$

(5) $\xi$是在数字产品$\tilde{X}_0$中加入水印的水印嵌入算法

$\xi:X\times W\times K\to X \quad \tilde{X}_w=\xi(\tilde{X}_0,\tilde{W})$

(6) D 为水印检测算法

$D:X\times K\to\{0,1\}$

$$D(\tilde{X},\tilde{W})=\begin{cases}1, & if \quad \tilde{W}\in W \quad (H_1)\\ 0, & otherwise \quad (H_0)\end{cases}$$

### 2.2 水印系统的 3 个组成部分

整个水印系统包括以下 3 部分。

(1) 水印生成

水印生成算法 G 应保证水印惟一性、有效性、不可逆性和图像相关性等属性。算法 G 可分为两部分：

收稿日期：2004-04-09。 基金项目：甘肃省科技攻关基金项目 (2GS033-A52-020)。
作者简介：袁占亭 (1961-)，男，陕西扶风人，教授，博士生导师，研究方向为信息安全、模式识别、信息管理和决策支持； 张秋余 (1966-)，男，河北辛集人，副教授，硕士生导师，研究方向为数据库、网络与信息系统、信息安全和软件工程； 陈宁，硕士生，研究方向为计算机网络与通信、信息安全和模式识别。

$G=ToR$

$R:K\to W,T:W\times X\times K\to W$

子算法$R$的输出为依赖于密钥$\vec{K}$的原水印$\vec{W}$。

子算法$T$修改原水印$\vec{W}$以得到与产品相关的水印$\vec{W}$，且应满足下列条件：

$$T(\vec{W},\vec{X}_0)\cong T(\vec{W},\vec{X}_w)\cong T(\vec{W},\vec{X}'_w)$$

其中，$\vec{X}_0$表示原产品，$\vec{X}_w$是加入水印的产品。若用$M$表示对数字产品的多媒体数据处理操作，则$\vec{X}'_w=M(\vec{X}_w),\vec{X}'_w\sim\vec{X}_w$。（“$\cong$”的含义：若$D(\vec{X},\vec{W}_1)=1\Rightarrow D(\vec{X},\vec{W}_2)=1$，则水印$\vec{W}_1$等价于$\vec{W}_2$，记为$\vec{W}_1\cong\vec{W}_2$）

(2) 水印嵌入

嵌入算法$\xi$需保证水印的不可知觉性和鲁棒性。嵌入过程把数字水印信号$\vec{W}=\{w(k)\}$嵌入到产品$\vec{X}_0=\{x_0(k)\}$中，一般水印嵌入规则可以描述为：

$$x_w(k)=x_0(k)\oplus h_0(k)\oplus w(k)$$

其中$\oplus$为某种叠加操作，$\vec{H}=\{h(k)\}$称为水印嵌入掩码。最简单的水印嵌入规则为

$$x_w(k)=x_0(k)+\alpha w(k)\qquad\text{(加法规则)}$$

$$x_w(k)=x_0(k)+\alpha x_0(k)w(k)\qquad\text{(乘法规则)}$$

变量$x$指采样强度/幅度（空域/时域）或是变换系数大小（变换域）。根据对水印的可觉察程度的不同要求，参数$\alpha$在各种数据采样中可能不同。

(3) 水印检测

水印检测算法应具有良好的可靠性和计算效率。水印检测器D可能发生两类错误：①数据中不存在水印，检测结果为存在水印；②数据中存在水印，检测结果为不存在水印。

上述错误发生的概率分别为虚警概率和漏报概率。

## 3 数字水印的鲁棒性

鲁棒性是衡量一种水印算法优劣的关键，它与数字水印的其它重要特征，如保真度、数据有效载荷以及安全性等有着密切的联系，它直接关系到水印技术在各种应用领域中的稳定性和可靠性。因此有必要对其进行详细的分析和研究。

### 3.1 鲁棒性概念

鲁棒性[2,7]是指不因多媒体文件的某种改动而导致隐藏信息丢失的能力。在第 2 节中提到的通用水印框架中，若记$\vec{Y}=M(\vec{X}_0)$及$\vec{Y}'=M(\vec{X}_w)$，则应满足的鲁棒性条件为：

$$D(\vec{Y},\vec{W})=1,\quad\forall\vec{Y}\sim\vec{X}_0$$

$$D(\vec{Y}',\vec{W})=0,\quad\forall\vec{Y}'\sim X_0$$

其中，符号“$\sim$”表示两者有相同的知觉外观。

### 3.2 影响鲁棒性的因素

水印鲁棒性与应用的目的类型无关，主要依赖于下面3个方面。

(1) 嵌入信息的数量[5]：该参数直接影响水印的鲁棒性。就同一种水印算法而言，要嵌入的信息越多，水印鲁棒性越差。

(2) 水印嵌入强度：该参数对应于水印的鲁棒性，它和水印不可见性[3]之间存在着冲突，因为增加鲁棒性就要增加水印嵌入强度，相应地会增加水印的可见性。为此，必须根据具体应用在两者之间进行折衷。

(3) 图像的尺寸和特性：图像的尺寸对嵌入水印的鲁棒性有直接影响。尽管非常小的含水印的图片的商用价值不大，但一种水印算法必须能从此图片中恢复出水印。另外，图像的特性也对水印的鲁棒性产生重要影响。

就拿图像水印而言，对扫描的自然图像具有高鲁棒性的方法在用于合成图像（如计算机产生的图像）时，鲁棒性大大削弱。

需要指出的是，鲁棒性水印与安全水印是有区别的。鲁棒水印能经受住传输过程中的常规信号处理，而安全水印则用来防止敌手的任何阻碍水印用途的攻击（如未经授权的嵌入、检测和去处等）。

由于在绝大多数应用中，若所嵌入的水印不可测，则水印不能实现其功能，因此鲁棒性是水印具有安全性的一个必要条件。

换句话说，如果使用常规信号处理就能消除水印，那么不能认为该水印是安全的。

总之，在水印作品传输的过程中可能会经受各种各样的处理操作，如空间滤波、有损压缩、数－模－数转换、模拟录制（如VHS或音频录制）、打印与扫描、回放与重录制、降噪和制式转换等，然而，对抗给定处理的鲁棒性常常会以损失一些计算花费、嵌入信息的数量、水印不可见性或对抗一些其它处理操作过程的鲁棒性为代价。

明智的做法是忽略在确定应用中那些不太可能的处理操作。例如，用来监视电视广告的视频水印需要经受住广播过程中的数－模转换、有损压缩等处理操作，但不需要经受住旋转、半调处理等操作。

### 3.3 实现鲁棒性的策略

要实现鲁棒性通常可采取两种策略[6]：一种是保证水印不被常规处理修改或细微修改。这种策略依赖于要在处理中找到某变换域，在此变换域中，一些数据项不会因处理受到影响；另一种策略是基于逆转失真效果的方法，这些方法允许水印因失真而被修改，但可在检测器或嵌入器中抵消这种修改。具体实现方法包括：

(1) 冗余嵌入，即将水印冗余的嵌入到几个系数中，即使其中一些系数被损坏，仍然可以检测到其余系数中的水印。它可提高对抗剪切滤波和加性噪声的鲁棒性。

冗余可存在于样品域、频域或处理中仅有部分信号失真的其它任何域。

(2) 扩频编码，它可大幅度降低信噪比进而降低可感知的人为因素的危险，其次，水印被分散到大量频率上还能使水印对许多常规信号失真具有鲁棒性。因此它提供了对抗滤波、加性噪声和剪切的一般鲁棒性。

(3) 在内容感知重要的成分里嵌入水印，确保对任何保持可接受保真度的处理过程的鲁棒性。

(4) 检测器失真补偿，如果检测器可以确定一个特定的处理已被用于一个作品（从它嵌入水印时起），那么检测器可以通过逆处理来弥补失真。

(5) 嵌入器失真补偿，有时能预测水印会遭受一小部分可能失真中之一。这种情形下，在嵌入过程中可以应用失真补偿[4]。

### 3.4 鲁棒性评估的描述

由 3.2 节知道制约鲁棒性的因素有多个，因此为了能对给定算法的鲁棒性进行合理评估，应该固定某些因素，也就是说，应该控制测试的环境。

表 1 给出了两种用于评价鲁棒性图表，以及可用于比较的变量和固定参数。鲁棒性可以由“位误码率”(bit-error) 来评估。

位误码率被定义为解码出的错误位数与全部嵌入数据位数之比。它也可用“检测误码率”(detection-error)来表征，即 1 减去位误码率的位数次方。

表 1　鲁棒性评估曲线对应参数情况

| 图表类型 | 参数 | | | |
|---|---|---|---|---|
| | 视觉质量 | 鲁棒性 | 攻击 | 嵌入比特数 |
| 鲁棒性—攻击曲线 | 固定 | 变化 | 变化 | 固定 |
| 鲁棒性—视觉质量曲线 | 变化 | 变化 | 固定 | 固定 |

(1) 鲁棒性对攻击强度曲线：它反映的是在给定视觉质量的前提下，位误码率或检测误码率与攻击强度之间的函数关系。

这种评价允许对水印鲁棒性进行直接比较，并且显示了水印系统对攻击的整体鲁棒性性能。

(2) 鲁棒性对视觉质量曲线：它反映了在给定的攻击强度下，位误码率或测试误码率与视觉质量之间的关系。此曲线可以用来决定在一定攻击强度和期望的误码率要求下可得到的最小视觉质量。

## 4　一种新的估计水印鲁棒性的算法

图 1 为一个采用盲检测器的水印模型。其中 m 表示要嵌入的信息；$w_a$ 表示由 m 映射的附加模板，它与载体作品 $c_o$ 的类型一致，维数相等；$c_w$ 为将 $w_a$ 加到载体作品 $c_o$ 上，产生的水印作品；$c_{wn}$ 为 $c_w$ 经历了某些处理操作得到的结果；$w_n$ 为从 $c_{wn}$ 减去载体所得到的带噪声的水印模型。

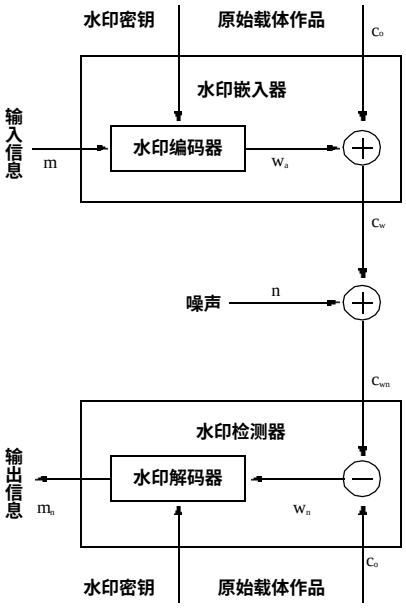


图 1　盲检测器的水印系统

根据以上模型，我们提出了一种估计图像水印鲁棒性的方法。其基本原理是通过对原始载体图像和水印载体图像所对应的矩阵中信息比特的聚合程度的变化进行计算和分析，来估计水印算法的鲁棒性的优劣。

具体算法可描述如下。

(1) 计算原始载体图像 $c_o$ 中影响图像视觉感知质量的信息比特数，记为 $C_{awnr}(c_o)$；

(2) 将 $n$ 维矩阵 $c_o$ 分成互不重叠的 $k$ 个 $m$ 维的矩阵块 $block_0$, $block_1$ … $block_{k-1}$，计算出每个图像块中影响图像感知质量的信息比特数，记为：$C_{awnr}(block_i), i=0,1,\cdots,k-1$ 并取其中的最大值，记为 $MAX_o(C_{awnr})$；

(3) 取 $\xi_o=\frac{MAX_o(C_{awnr})}{C_{awnr}(C_O)}$，我们称它为原始载体图像的特征因子；

(4) 用与(2)完全相同的方法计算出 $MAX_w(C_{awnr})$，进而计算出水印载体图像的特征因子 $\xi_w=\frac{MAX_w(C_{awnr})}{C_{awnr}(C_O)}$，并取 $\lambda=\frac{\xi_w}{\xi_o}$，我们称其为水印算法的鲁棒性因子。

根据 $\lambda$ 的值可定性判断水印算法的优劣，即 $\lambda$ 的值越小，水印算法的鲁棒性越好。

该算法之所以成立是因为它和扩频通信技术具有相同的理论依据，$\lambda$ 的值越小，表明水印信号的能量被较均匀地分布到整个载体图像中，说明对应的水印算法不但具有较高的保真度且具有较强的抵御常规信号处理 (如剪切、加性噪声等) 的鲁棒性。

## 5　结束语

鲁棒性的优劣直接关系到水印技术应用的可靠性和稳健性。

本文在介绍通用数字水印框架的基础上对水印鲁棒性的重要性、影响因素、实施的基本策略和具体方法以及评估鲁棒性的方法做了全面的分析，并提出了一种粗略估计水印鲁棒性的新方法。

## 参考文献:


[1] 汪小帆, 戴跃伟. 信息隐藏技术、方法与应用[M]. 北京: 机械工业出版社, 2001.

[2] Ingemar J Cox, Matt L Miller,Jeffrey A Bloom. Watermarking applications and their properties[A]. Int Conf on Information Technology'2000, 2000.

[3] Ingemar J Cox, Matt L Miller. A review of watermarking and the importance of perceptual modeling[C]. Proc of Electronic Imaging'97, 1997.

[4] 考克斯(Cox,I J ). 数字水印[M]. 北京: 电子工业出版社, 2003.

[5] 胡军全, 黄继武, 张龙军, 等. 结合数字签名和数字水印的多媒体认证系统[J]. Journal of Software, 2003, 14(6).

[6] Voyatzis G, Pitas I. Embedding robust logo watermarks in digital images[C]. Proc of DSP'97, 1997. 213-216.

[7] 许剑峰, 黎绍发. 基于可信赖第三方的鲁棒性的图像水印方案[J]. 计算机工程与设计, 2003, 24(10):73-74.