计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
42(7):1093~1099, 2005

# 数字水印技术综述

尹 浩 林 闯 邱 锋 丁 嵘
(清华大学计算机科学与技术系 北京 100084)
(h-yin@mail.tsinghua.edu.cn)

# A Survey of Digital Watermarking

Yin Hao, Lin Chuang, Qiu Feng, and Ding Rong
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

**Abstract** Digital watermarking, the technology of embedding special information into multimedia data, is a topic that has recently gained increasing attention all over the world. The watermark of digital images, audio, video, and other media products in general has been proposed for resolving copyright ownership and verifying the integrity of content. The characteristics and applications of watermark techniques are first introduced, and then the basic concepts and evaluation criteria are expatiated. For further understanding, the watermark techniques from the various aspects are classified and some conventional watermark techniques and algorithms are analyzed in detail. At the same time, their security and performance are compared. Finally, the possible research direction of digital watermark technology are pointed out.

**Key words** digital watermark; multimedia security; copyright protection

**摘 要** 数字水印作为一种将特殊信息嵌入媒体数据的技术,近年来已成为国内外研究的热点并有着广泛的应用前景. 通常数字水印被应用于数字图像、音频、视频以及其他媒体产品上以进行版权保护和验证多媒体数据的完整性. 首先介绍了数字水印技术的特点和应用领域,并对其基本原理和评价标准进行了阐述,同时对数字水印的各种算法进行了分类研究与深入分析,并对不同算法进行了安全性与性能的横向比较,最后指出了数字水印今后的研究方向.

**关键词** 数字水印;多媒体安全;版权保护

**中图法分类号** TP309.7

## 1 引 言

随着数字技术和因特网的发展,图像、音频、视频等形式的多媒体数字作品纷纷在网络上发布,其版权保护与信息完整性保证逐渐成为迫切需要解决的一个重要问题. 数字水印(digital watermarking)技术作为信息隐藏技术研究领域的重要分支,是实现多媒体版权保护与信息完整性保证的有效方法,目前也正成为信息领域的一个研究热点[1,2].

## 2 特点、分类及其应用

### 2.1 基本特点

(1) 不可见性(imperceptibility)

数字水印的嵌入不应使得原始数据发生可感知的改变,也不能使得被保护数据在质量上发生可以感觉到的失真.

收稿日期:2004-05-17;修回日期:2004-12-06
基金项目:国家自然科学基金项目(60372019,90104002,90412012,60473086);中国博士后基金项目(2003034152);国家"九七三"重点基础研究发展规划基金项目(2003CB314804)

(2) 鲁棒性(robustness)

当被保护的数据经过某种改动或者攻击(如传输、编码、有损压缩等)以后,嵌入的水印信息应保持一定的完整性,并能以一定的正确概率被检测到.

(3) 安全性(security)

数字水印应该难以被伪造或者加工. 并且,未经授权的个体不得阅读和修改水印,理想情况是未经授权的客户将不能检测到产品中是否有水印存在.

(4) 可证明性

在实际的应用过程中,可能多次加入水印,那么数字水印技术必须能够允许多重水印嵌入被保护的数据,而且每个水印均能独立地被证明.

### 2.2 分 类

(1) 按照应用媒体分为文本、图像、音频和视频.

(2) 按照水印特点,分为可见水印和不可见水印.不可见水印是最常用的水印技术,它利用了人类视觉系统的特点,使得隐藏在数据中的水印无法通过肉眼分辨出来. 它可以分为脆弱水印、半脆弱水印和稳健水印.

(3) 按照水印处理过程,由图 1 可以看到分为生成水印、嵌入水印和检测水印,而其中每一种又有不同的分类.

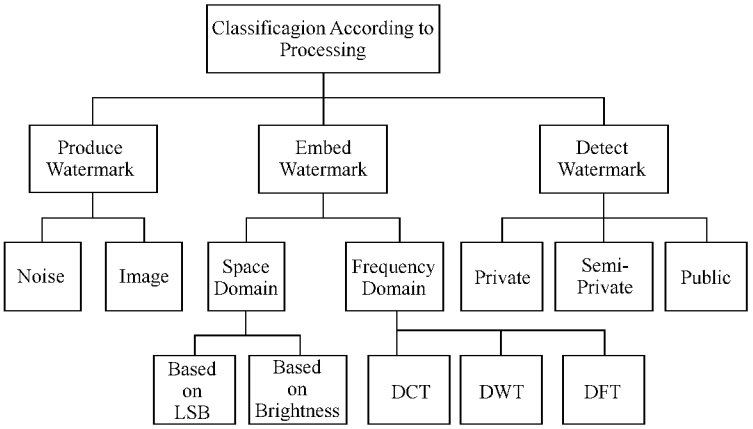


Fig. 1 Watermarking classification according to processing.

图 1 数字水印按照处理过程分类

### 2.3 应 用

数字水印主要应用在以下几个方面[1~10]:

(1) 版权保护

数字作品的所有者可用密钥产生水印,并将其嵌入原始数据,然后公开发布其水印版本作品. 当该作品被盗版或出现版权纠纷时,所有者即可从被盗版作品中获取水印信号作为依据,从而保护其合法权益.

(2) 数字指纹

为避免数字作品未经授权被拷贝和发行,版权所有人可以向分发给不同用户的作品中嵌入不同的水印以标识用户的信息 . 该水印可根据用户的序号和相关的信息生成,一旦发现未经授权的拷贝,就可以根据此拷贝所恢复出的指纹来确定它的来源.

(3) 认证和完整性校验

通常采用脆弱水印. 对插入了水印的数字内容进行检验时,须用惟一的与数据内容相关的密钥提取出水印,然后通过检验提取出的水印完整性来检验数字内容的完整性. 其优点在于认证同内容密不可分,因此简化了处理过程.

(4) 访问控制

利用数字水印技术可以将访问控制信息嵌入到媒体中,在使用媒体之前通过检测嵌入到其中的访问控制信息,以达到访问控制的目的,它要求水印具有很高的鲁棒性.

(5) 信息隐藏

数字水印可用于作品的标识、注释、检索信息等内容的隐藏,这样不需要额外的带宽,且不易丢失. 另外,数字水印技术还可以用于隐蔽通信,这将在国防和情报部门得到广泛的应用.

## 3 基本原理和评价标准

### 3.1 常规的嵌入检测框架

图 2 所表示的是常规水印嵌入模型,其功能是根据密钥 Key 生成水印信号 $W$,通过一定的方法加入原始数据中,得到嵌入了水印的作品. 在水印信

号生成过程中,通常是需要原始数据的,其作用是使生成的水印信号与原始数据相关,即在不同的数据中嵌入的水印信号各不相同.

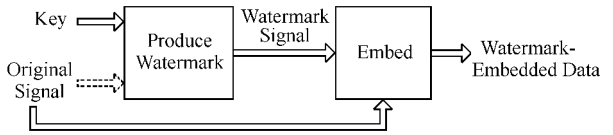


Fig. 2　Normal watermark-embedding model.

图2　常规的水印嵌入模型 original

图3是常规的水印检测模型,其功能是根据KEY生成水印信号 $W$,然后与待测数据进行水印信号相似性检测,判断是否存在水印.生成水印信号是否使用待测数据需与水印嵌入过程中的生成方法一致.一些水印技术(如私有水印等)中,检测过程需要使用原始数据,以便有效解决一些水印鲁棒性问题[3],但这同时也带来了一些额外的开销和安全隐患.

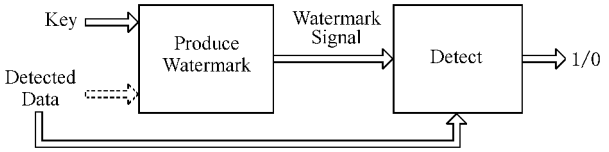


Fig. 3　Watermark detection model.

图3　水印检测模型

常规的数字水印技术框架可以定义为六元组[1]$(\boldsymbol{X},\boldsymbol{K},\boldsymbol{W},G,E,D)$:

$\boldsymbol{X}$ 表示未加入水印的原始数据.

$\boldsymbol{K}$ 表示水印密钥(watermark key),常由标识数字序列(例如整数序列等)组成.

$\boldsymbol{W}$ 表示由数据序列 $\boldsymbol{X}$ 和水印密钥 $\boldsymbol{K}$ 生成的水印信号序列,其定义如下:

$$\boldsymbol{W} = \{w(k) \mid w(k) \in U, k \in \hat{W}^d\}. \quad (1)$$

水印信号可为二值的形式[4~6],即水印信号序列中的每个值 $w(k)$,其取值范围 $U = \{0,1\}$ 或 $\{-1,1\}$;也可以高斯噪声的形式[7,8]出现. $\hat{W}^d$ 表示水印信号空间,而 $d$ 表示其维数,$d=1,2,3$ 分别表示音频、图像和视频水印.

$G$ 表示从数据序列 $\boldsymbol{X}$ 和水印密钥 $\boldsymbol{K}$ 生成水印信号 $\boldsymbol{W}$ 的算法:

$$\boldsymbol{W} = G(\boldsymbol{X},\boldsymbol{K}). \quad (2)$$

二值形式的水印信号通常基于伪随机数产生器或者混沌系统;而高斯伪噪声信号或者m-序列则可以通过提供很长的不相关信号序列来产生,以保证其足够的安全性.另外,生成的水印可能需要进一步的变换,以便更适合于嵌入到数据中.为了便于分析,可将 $G$ 分解为两个部分:

$$G = T \circ R, \quad (3)$$

其中,

$$\widetilde{\boldsymbol{W}} = R(\boldsymbol{K}), \boldsymbol{W} = T(\widetilde{\boldsymbol{W}},\boldsymbol{X}).$$

第1部分 $R$ 表示从密钥 $\boldsymbol{K}$ 生成原始水印的变换过程,整个过程仅依赖于 $\boldsymbol{K}$.如果 $R$ 基于随机数生成器,则 $\boldsymbol{K}$ 可直接映射为生成随机数所需的种子(seed);而如果基于混沌系统,$\boldsymbol{K}$ 则可通过一些简单变换以成为混沌系统的初始条件.上述两种情况 $R$ 都满足了密钥的惟一性,并且生成的 $\widetilde{\boldsymbol{W}}$ 是 $\boldsymbol{K}$ 的合法水印;另外,企图通过 $R$ 的逆变换来求得密钥 $\boldsymbol{K}$ 实际上是不可行的.

第2部分 $T$ 是可选的处理过程,表示将 $R$ 生成的原始水印修改为与被保护数据内容相关的水印,$T$ 只看重数据的一些显著的特征,比如数据在处理过程中比较鲁棒不易丢失的那些特征等.如果在大量数据中嵌入同样的水印,攻击者可以通过统计的方法将数据进行叠加,来估计出水印信号[9],而通过数据相关的处理,即使采用相同的原始水印,对不同的数据得到的水印也不相同,因此可以避免此类攻击.

$E$ 表示将水印信号 $\boldsymbol{W}$ 嵌入数据序列 $\boldsymbol{X}$ 得到加密后的序列 $\boldsymbol{X}_w$ 的算法:

$$\boldsymbol{X}_w = E(\boldsymbol{X},\boldsymbol{W}) = \boldsymbol{X} + af(\boldsymbol{X},\boldsymbol{W}), \quad (4)$$

其中 $\boldsymbol{X} = \{x(k)\}$,$a$ 为水印强度,$f$ 为 $\boldsymbol{X}$ 与 $\boldsymbol{W}$ 的某种函数关系,最常用的水印嵌入算法如下:

加法规则 $x_w(k) = x(k) + aw(k)$. (5)

乘法规则 $x_w(k) = x(k) + ax(k)w(k)$. (6)

为了保证在不可见的前提下,尽可能提高嵌入水印的强度,$a$ 的选择必须考虑图像的性质和视觉系统的特性.

$D$ 表示水印检测算法:

$$D(\boldsymbol{X},\boldsymbol{K}) = \begin{cases} 1, & \boldsymbol{W} \text{ 存在}, \\ 0, & \boldsymbol{W} \text{ 不存在}. \end{cases} \quad (7)$$

不论水印是否受到攻击而造成失真,或者水印根本就不存在,都可以通过相似性测量来检测出来.有多种办法可以度量原始水印和提取的水印之间的相似程度,最常用的是基于相关性的测试.先用密码和待检测的图像算出水印 $\boldsymbol{W}^*$,通常情况下,提取出的水印 $\boldsymbol{W}^*$ 与原始水印 $\boldsymbol{W}$ 不相等,然后用下面的公式进行计算:

$$sim(\boldsymbol{W}^*,\boldsymbol{W}) = \frac{\boldsymbol{W}^* \cdot \boldsymbol{W}}{\sqrt{\boldsymbol{W}^* \cdot \boldsymbol{W}}}. \quad (8)$$

设定阈值为 $T$,当满足下面不等式时,$\boldsymbol{W}^*$ 与 $\boldsymbol{W}$ 匹配:

$$sim(\boldsymbol{W}^*,\boldsymbol{W}) > T. \tag{9}$$

$T$ 的选择要基于一定的虚警概率和漏警概率.检测过程可能包含两个错误,一是实际没有水印,却检测出有水印;二是实际有水印,却没有检测到水印. $T$ 减小,漏警概率降低而虚警概率提高;$T$ 增大,则虚警概率降低而漏警概率提高.

### 3.2 攻击测试与性能评价

(1) 攻击

在实际应用中,数字水印会面临各种问题,包括数据处理和人为攻击所带来的破坏,大致分类如下:

① 一般信号处理,包括滤波、平滑、增强、有失真压缩等;

② 几何变化,包括旋转、缩放、分割等;

③ 诱惑攻击,即试图通过伪造原始图像和原始水印来迷惑版权保护,也称 IBM 攻击;

④ 删除攻击,即针对某些水印方法通过分析水印数据,估计图像中的水印,然后将水印从图像中分离出来并使水印检测失效.

(2) 评价标准

水印算法的评估有多种客观的评估标准,但主要有以下 3 种评价标准:

① 信噪比 $SNR$ 和峰值信噪比 $PSNR$

在实验中,我们使用信噪比($SNR$)和峰值信噪比($PSNR$)作为嵌入水印后图像质量的评估标准,它是一种客观评价标准. 信噪比($SNR$)和峰值信噪比($PSNR$)分别定义如下(单位分贝,dB):

$$SNR = -10\lg\frac{\sigma^2}{D}, \tag{10}$$

$$PSNR = -10\lg\frac{M^2}{D}, \tag{11}$$

其中:

$$\sigma^2 = \frac{1}{N}\sum_{i=0}^{N-1}(x_i-\bar{x})^2, \quad \bar{x} = \frac{1}{N}\sum_{i=0}^{N-1}x_i, \tag{12}$$

$$D = \frac{1}{N}\sum_{i=0}^{N-1}(x_i-\hat{x}_i)^2. \tag{13}$$

$x_i$ 表示原图的像素值,$\hat{x}_i$ 表示输出图像的像素值,$N$ 表示图像的像素个数,$[0,M-1]$ 为图像像素值的取值范围.

② 水印容量[11]

在给定水印(二值型或高斯型)和图像质量标准的前提下,某些水印系统可以测出水印的最大长度和强度. 水印容量越大,所含版权信息越多,不可见性会随之下降.

③ 鲁棒性

数字水印算法的鲁棒性常用攻击测试来进行评价,常见攻击测试包括:低通滤波、色彩量化、按比例缩放、剪切、旋转、对称或非对称剪切($X$,$Y$ 方向)、对称或非对称行和列移动、普通线形几何变换、JPEG 压缩、小波压缩等[12]. 除了上述基本的攻击测试,近年来又出现了统计平均攻击和引发多著作权问题的多重水印攻击[13,14].

总之,在统一了测试方法和评估标准以后,水印算法的作者只需提供一份测试结果列表,其他研究者就能对算法的性能产生较为全面的认识,有利于对算法的深入研究及推广.

## 4 数字水印典型算法

近年来,国际上数字水印技术的研究发展很快,新技术新算法层出不穷. 水印算法大致可以分为两类:即空域水印和频域水印. 后者通常也称为变换域水印,目前很多新的水印算法都是基于变换域的. 下面对一些典型的算法进行介绍.

### 4.1 空域算法

(1) Schyndel 算法[15,16]

Schyndel 算法提出了一些关于水印的重要概念和鲁棒水印检测的通用方法,即相关性检测方法. 该算法首先将一个密钥输入一个 m-序列(maximum-length random sequence)发生器来产生水印信号,然后排列成二维水印信号,按像素点逐一嵌入到原始图像像素值的最低位上. 其中,m-序列是由一些初始向量按照 Fibonacci 递归数列的关系运算生成的,也可以用线性移位寄存器实现. 如果每个向量的长度为 $n$,或移位寄存器的级数为 $n$,则生成的 m-序列长度最大为 $2^n-1$. m-序列的自相关函数和频谱分布的特点类似于随机高斯噪声. 检测时,通过计算 m-序列和水印图像行的相关函数来判断是否存在水印. 由于 Schyndel 算法将水印信号安排在了像素点的最低位上,它是不可见的. 但基于同样的原因,水印信息很容易为滤波、图像量化、几何变形的操作破坏,因此是不鲁棒的.

(2) Patchwork 算法[3]

Patchwork 算法是通过改变图像数据的统计特性将信息嵌入到像素的亮度值中. Patchwork 算法的方法是随机选择 $N$ 对像素点$(a_i,b_i)$,这些随机选取的两个像素点的差值是以 0 为中心的高斯分布.然后将点 $a_i$ 的亮度值加 1,点 $b_i$ 的亮度值减 1,这样来改变分布的中心,并且使得整个图像的平均亮度保持不变. 最后采用统计的方法来对水印进行

检测.为了抵抗诸如有损压缩以及滤波的处理,它将像素点对扩展成小块的像素区域(patch),增加一个 patch 中的所有像素点的亮度值,同时减少对应另外一个 patch 中所有像素点的亮度值.这种算法对抵御有损压缩编码(JPEG)、剪裁攻击和灰阶校正非常有效.但其缺陷在于嵌入的水印信息少,对仿射变换敏感,对多拷贝联合攻击抵抗力比较脆弱.

### 4.2 频域算法

(1) 扩展频谱通信技术

扩展频谱通信[7](spread spectrum communication)技术原理为:先计算图像的离散余弦变换(DCT),然后将水印叠加到 DCT 域中幅值最大的前 $L$ 个系数上(不包括直流分量),通常为图像的低频分量.若 DCT 系数的前 $L$ 个最大分量表示为 $\boldsymbol{D}=\{d_i\}$, $i=1,\cdots,L$,水印是服从高斯分布的随机实数序列 $\boldsymbol{W}=\{w_i\}$, $i=1,\cdots,L$,那么水印的嵌入算法为 $d_i^*=d_i+ad_iw_i$,其中常数 $a$ 为尺度因子,控制水印添加的强度.然后用新的系数做反变换得到水印图像 $\boldsymbol{X}^*$.解码函数则分别计算原始图像 $\boldsymbol{X}$ 和水印图像 $\boldsymbol{X}^*$ 的离散余弦变换,并提取嵌入的水印 $\boldsymbol{W}^*$,再做相关检验 $sim(\boldsymbol{W}^*,\boldsymbol{W})=\dfrac{\boldsymbol{W}^*\cdot\boldsymbol{W}}{\sqrt{\boldsymbol{W}^*\cdot\boldsymbol{W}}}$,以确定水印的存在与否.该方法即使当水印图像经过一些通用的几何变形和信号处理操作而产生比较明显的变形后仍然能够提取出一个可信赖的水印.

(2) NEC 算法

NEC 算法[7]由 NEC 实验室的 Cox 等人提出,在数字水印算法中占有重要地位.其工作原理是,首先由作者的标识码和图像的 Hash 值等组成密钥,以该密钥为种子来产生伪随机序列,该序列具有高斯 $N(0,1)$ 分布.再对图像做 DCT 变换,用该伪随机高斯序列来调制(叠加)图像除直流(DC)分量外的 1000 个最大的 DCT 系数.该算法具有较强的鲁棒性、安全性、透明性等.由于采用特殊的密钥和不可逆的水印生成方法,因此可以有效防止 IBM 攻击.而且该算法还提出了增强水印鲁棒性和抗攻击算法的重要原则,文献[6]建议水印信号应该嵌入到图像频域中可见性最主要的部分,这样可以增强抵抗常规信号处理和几何失真,以提高检测出水印的概率.另外,待嵌入的水印信号要由独立同分布随机实数序列构成,并且该实数序列应该具有高斯分布 $N(0,1)$ 的特征.

(3) 生理模型算法

人的生理模型包括人类视觉系统 HVS 和人类听觉系统 HAS.利用生理模型的基本思想均是利用从视觉或听觉模型导出的 JND(just noticeable difference)描述来确定在图像或声音的各个部分所能容忍的数字水印信号的最大强度,从而能够避免破坏视觉或者听觉的质量.也就是说,利用生理模型来确定与数据相关的调制掩模,然后再利用其来嵌入水印.这一方法同时具有好的透明性和鲁棒性.

(4) 压缩域算法

基于 JPEG,MPEG 标准的压缩域数字水印系统,其水印检测与提取可直接在压缩域数据中进行,节省了完全解码和重新编码过程,因此在数字电视广播及 VOD 中有很大的实用价值[17~22].输入的 MPEG-2 数据流可以分为数据头信息、运动向量和 DCT 编码信号块这 3 个部分,常见的方案都主要是对 DCT 编码信号块进行改变,如 H&G 算法[17,18].

### 4.3 主要算法比较

表 1 对一些常见的数字水印算法,对其不可见性、鲁棒性、嵌入量以及复杂程度进行了分类比较,以便进一步地研究.总体来说,频域水印的不可见性要比空域水印好,且抗攻击能力很强,但是嵌入量较小,计算更为复杂.实际应用中,需要选择合适的算法,以适应不同的需求.

**Table 1 Comparison Between Main Algorithms**

**表 1 主要算法比较**

| Classification | | Algorithm | Imperceptibility | Resistibility | Embedding Quantity | Complexity Degree |
|---|---|---|---|---|---|---|
| Spatial Domain Watermarking | Based on LSB | Schyndel Algorithm | Insert into LSB, good imperceptibility | Weak resistibility for filter, image quantization and geometric distortion. | Large | Very Low |
| | Based on Brightness | Patchwork Algorithm | Modify the distribution of brightness difference, good imperceptibility | Effective for lossy compression and coding, shearing attack and gray correction, fragile for affine transform and multi-copy joint attack. | The distribution of brightness difference of $N$ pixels pairs represented only one bit, little watermark embedded data. | Low |

续 表

| Classification | | Algorithm | Imperceptibility | Resistibility | Embedding Quantity | Complexity Degree |
|---|---|---|---|---|---|---|
| Frequency Domain Watermarking | Based on DCT | Spread-Spectrum Communication | Good imperceptibility, but the watermark in different frequency has the same intensity. | Robust to geometric distortion and signal processing. | Embedded in the DCT coefficients, Large number of embedded data. | High |
| | | NEC Algorithm | Good imperceptibility, but the watermark in different frequency has the same intensity. | Robust to geometric distortion, signal processing and IBM attack. | Embedded in the DCT coefficients, Large number of embedded data. | Higher than the Spread-spectrum communication. |
| | | Physiological Model Algorithm | Good imperceptibility, but the watermark in different frequency has the same intensity. | Robust to geometric distortion and signal processing. | Embedded in the DCT coefficients, Large number of embedded data. | High |
| | | Compression Field Algorithm | Good imperceptibility. | Robust to video compression and shearing operation. Some practical algorithms have bad transparency on the QoS control. | Embedded in the DCT coefficients, Large number of embedded data. | Low, DCT/IDCT is Avoided. |
| | Based on DWT | Multi-Resolution Decomposition Algorithm | Good imperceptibility. | Robust to compression and image processing. | Embedded in the sub-wave band, Large number of embedded data. | Higher than DCT transform for block image. |
| | Based on DFT | Algorithm Presented by Ruanaidh | Good imperceptibility. | Robust to compression and image processing. | Embedded in the phase information of every block, few embedded data. | Higher |

## 5 结 论

数字水印是近几年来国际学术界兴起的一个前沿研究领域,作为在信息时代下进行数字产品版权保护的新技术,它可以确定版权所有者,识别购买者或者提供关于数字内容的其他附加信息,并将这些信息以人眼不可见的形式嵌入在多媒体信息中. 在数字水印技术中,水印嵌入算法一直都是人们关注的焦点,而对不可见的鲁棒水印和嵌入噪声的水印的研究,都是最常见的课题. 频域比空域应用得更多更广,尤其是基于 DCT 变换的算法已经得到了广泛的应用. 但最近基于小波变换的嵌入算法因其具有多重分辨率的特点,而日益变得流行起来.

由于目前数字水印技术难以解决串谋攻击、机会攻击以及解释攻击问题,使得数字水印在版权保护、访问与拷贝控制、数字指纹等方面的应用受到了很大的限制,许多研究者正致力于上述问题的解决. 另外,对数字水印算法的可靠性和性能的评价需要有更标准的方法,水印理论也需要更加完善,可以预见数字水印技术将很可能成为多媒体安全领域的技术基础.

## 参 考 文 献


1 G. Voyatzis, I. Pitas. The use of watermarks in the protection of digital multimedia products. Proceedings of the IEEE, 1999, 87(7):1197~1207

2 Christine I. Podilchuk, Edward J. Delp. Digital watermarking: Algorithms and applications. Signal Processing Magazine, 2001, 14(4):33~46

3 Ingemar J. Cox, J. P. Linnartz. Some general methods for tampering with watermarks. IEEE Journal on Selected Areas in Communication, 1998, 16(4):587~593

4 W. Bender, D. Gruhl, N. Morimoto, *et al*. Techniques for data hiding. IBM System Journal, 1996, 35(3&4):313~336

5 R. B. Wolfgang, E. J. Delp. A watermark for still images. IEEE Int'l Conf. Image Processing, Lausanne, Switzerland, 1996

6 A. Z. Tirkel, C. F. Osborne, T. E. Hall. Image and watermark registration. Signal Processing, 1998, 66(3):373~383

7 Ingemar J. Cox, Joe Kilian, F. Thomason Leighton, *et al*. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Processing, 1997, 6(12):1673~1687

8 C. I. Podilchuk, W. Zeng. Perceptual watermarking of still images. IEEE Workshop Multimedia Signal Processing, Princeton NJ, 1997

9 S. Voloshynovskiy, S. Pereira, T. Pun, *et al*. Attacks on digital watermarks: Classification, estimation-based attacks and

benchmarks. IEEE Communications Magazine, 2001, 39(8): 118～126
10 Lee Sin-Joo, Jung Sung-Hwan. A survey of watermarking techniques applied to multimedia. IEEE Int'l Symposium Electronics, Pusan, Korea, 2001
11 Yu Nenghai, Cao liangliang, Fang Wen, *et al*. Practical analysis of watermarking capacity. Int'l Conf. Communication Technology Proceedings, Beijing, 2003
12 Liu Tong, Qiu Zhengding. Attacks and evaluation in image digital watermarking. Information and Control, 2001
13 S. Craver, N. Memon, B. L. Yeo, *et al*. On the invertibility of invisible watermarking techniques. IEEE Int'l Conf. Image Processing, Washington, CA, 1997
14 S. Craver, N.Memon, *et al*. Can invisible watermarks resolve rightful ownerships. IBM, Tech. Rep.: RC 20509, 1996
15 R. G. van Schyndel, A. Z. Tirkel, C. F. Osborne. A digital watermark. Int'l Conf. Image Processing, Austin, Texas, 1994
16 C. T. Hsu, J. L. Wu. Hidden digital watermarks in images. IEEE Trans. Image Processing, 1999, 8(1): 58～68
17 F. Hartung, B. Girod. Digital watermarking of MPEG-2 coded video in the bitstream domain. The 1997 IEEE Int'l Conf. Acoustics, Speech, and Signal Processing, Munich, Germany, 1997
18 F. Hartung, B. Girod. Digital watermarking of uncompressed and compressed video. Signal Processing (Special Issue on Copyright Protection and Access Control for Multimedia Services), 1998, 66(3): 283～301
19 G. C. Langelaar, R. L. Lagendijk, J. Biemond. Real-time labeling methods for MPEG compressed video. The 18th Symp. Information Theory in the Benelus, Veldhoven, Netherlands, 1997
20 F. Jordan, M. Kutter, T. Ebrahimi. Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video. Tech. Rep.: ISO/IEC Doc. JTC1/SC29/WG11 MPEG97/M2281, 1997
21 Cheng Hui, M. A. Isnardi. Spatial temporal and histogram video registration for digital watermark detection. The 2003 Int'l Conf. Image Processing, Barcelona, 2003
22 Z. H. Wei, P. Qin, Y. Q. Fu. Perceptual digital watermark of images using wavelet transform. IEEE Trans. Consumer Electronics, 1998, 44(4): 1267～1273

**Yin Hao**, born in 1974. Assistant researcher. Mainly researches on the multimedia communication, network QOS control and security.
**尹浩**,1974 年生,助理研究员,主要研究方向为多媒体通信与安全、网络性能评估与 QOS 控制.

**Lin Chuang**, born in 1948. Professor and Ph. D. supervisor. His main research interests are computer network, performance evaluation, stochastic Petri net, logic deduce and inference system.
**林闯**,1948 年生,教授,博士生导师,主要研究方向为计算机网络、系统性能评价、随机 Petri 网、逻辑推演和推理系统.

**Qiu Feng**, born in 1982. Master candidate. His main research interest is multimedia security.
**邱锋**,1982 年生,硕士研究生,主要研究方向为多媒体安全.

**Ding Rong**, born in 1975. Post Ph. D. His main research interests are video compression and recognition.
**丁嵘**,1975 年生,博士后,主要研究方向为视频压缩及识别.

**Research Background**

This paper is based on the research on an application-supported video secure transmission system, which is supported by the Natural Science Foundation (Grant No.60473086). With the development of the digital technology and the Internet, image, audio, video and so many kinds of multimedia digital production have been published in the Internet, then the copyright protection and information integrality guarantee has become important problems needed to be resolved. Digital watermarking technology, as an important branch of information security technology research fields, is an efficient method to realize the multimedia copyright protection and information integrality guarantee, and has become a research point in information fields. We try to design a media-dependent scheme to guarantee the security of video delivery, in this scheme, key information will be embedded in the host video, and delivered to the clients. How to design a reliable and efficient data embedding algorithm is a challenge. We hope to find some valuable information from the watermark research work. So to conduct a good survey on current watermark work is very important for our further work and is also very valuable to the related research work.

This paper firstly introduces the characteristics and applications of watermarking, and the basic concepts and evaluation criteria are expatiated. For further understanding, it then classifies the watermark techniques from the various points of view, analyzes some existing watermark techniques and algorithms in detail, and compares their security and performance. Finally, it briefly introduces the direction of digital watermarking technology development.