

# 数字视频水印技术综述

刘敏

(泉州财贸职业技术学校, 福建 泉州 362000)

**摘要:** 介绍了水印技术的定义及基本框架, 并对其理论基础和评价标准进行了阐述, 对数字水印的各种算法进行了分类研究与深入分析, 并对不同视频水印嵌入和提取方案进行了比较, 同时分析了人类视觉系统对水印可见性的影响, 最后指出了数字水印的应用领域及今后的研究方向。

**关键词:** 数字水印; 版权保护; 水印算法; 多媒体安全

中图分类号: TP309.2

文献标识码: A

文章编号: 1674-7720(2012)07-0006-05

## A survey of digital video watermarking

Liu Min

(Quanzhou Finance and Commerce Vocational School, Quanzhou 362000, China)

**Abstract:** 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 definition and basic framework of watermark techniques are first introduced, and then the basic theoretical 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, and their scheme of video watermarking embedding and extraction are compared. At the same time, the influence of human visual system to watermark visibility is analyzed. Finally, the application field and possible research direction of digital watermark technology is pointed out.

**Key words:** digital watermark; copyright protection; watermarking algorithm; multimedia security

随着网络和多媒体技术的发展, 越来越多的媒体文件(包括图像、音频和视频)转化成了数字形式, 并广泛地分布在网络上。因此, 知识产权的保护问题就成为了如今的关键问题。数字水印(Digital Watermarking)技术<sup>[1]</sup>的提出正是为了识别数字产品的所有权及分布途径问题。作为信息隐藏技术研究领域的一个重要分支, 数字水印可以实现多媒体版权保护和信息完整性验证, 目前也正成为信息安全领域的一个研究热点<sup>[2-3]</sup>。

### 1 数字水印的定义与框架模型

数字水印技术是将一个不可见的(诸如版权信息或验证信息等)标志嵌入到数字媒体中, 用于证明作品的所有权, 起到版权保护的作用。该标志具有不可感知性, 能抵抗试图破坏或者移除水印信息的恶意攻击。

根据信号处理理论, 数字水印可以看作在载体对象的背景下, 附加一个类似水印的弱信号。根据数字通信理论, 数字水印可以理解为应用扩频技术等通信手段, 在一个宽带信道(载体)上传输一个窄带信号(水印)。

一般地, 数字水印系统包括水印嵌入器和水印检测器<sup>[4]</sup>。水印嵌入器需要嵌入原始水印信息(密钥信息)和含水印的数字作品(载体作品), 其输出结果为含水印的数字产品。水印检测器需要嵌入含水印的数字产品。当提取水印时, 水印检测器根据需要确定是否包含原始载体或原始水印信息。图1为数字水印系统的基本框架图<sup>[4]</sup>。可以定义为九元体 $(M, I, W, K, G, Em, At, D, Ex)$ , 分别定义如下:

- (1)  $M$  表示全部的 secret 信息  $m$  的集合;
- (2)  $I$  表示被保护的原始数字作品  $I$  的集合;
- (3)  $W$  表示全部的水印信号  $w$  的集合;
- (4)  $K$  表示水印密钥信息  $k$  的集合;
- (5)  $G$  表示使用 secret 信息  $m$ 、密钥  $k$  和数字作品  $I$  生成的水印算法, 即:

$$G: M \times I \times K \rightarrow W, w = G(m, I, k) \quad (1)$$

数字产品  $I$  可不参与水印的生成过程, 因此产品  $I$  与水印  $w$  用虚线连接。

## 综述与评论 Review and Comment

(6)  $E_m$  表示将水印  $w$  嵌入到数字产品  $I$  中的嵌入算法, 即:

$$E_m: I \times W \rightarrow I', I' = E_m(I, w) \quad (2)$$

$I$  为原始作品,  $I'$  为含水印作品。将密钥包含在嵌入算法中以提高安全性。

(7)  $A_t$  表示对含水印作品的攻击算法, 即:

$$A_t: I \times K \rightarrow \hat{I}, \hat{I} = A_t(I', K') \quad (3)$$

其中,  $K'$  表示伪造的密钥,  $\hat{I}$  是被攻击后含水印的作品。

(8)  $D$  表示水印检测算法, 即:

$$D: I \times K \rightarrow \{0, 1\}, D(\hat{I}, K) = \begin{cases} 1, & \text{如果 } \hat{I} \text{ 中存在 } w(H_1) \\ 0, & \text{如果 } \hat{I} \text{ 中不存在 } w(H_0) \end{cases} \quad (4)$$

其中,  $H_1$ 、 $H_0$  代表二值假设, 表示水印是否存在。

(9)  $E_x$  表示水印提取算法, 即:

$$E_x: I \times K \rightarrow W, w' = E_x(\hat{I}, K) \quad (5)$$

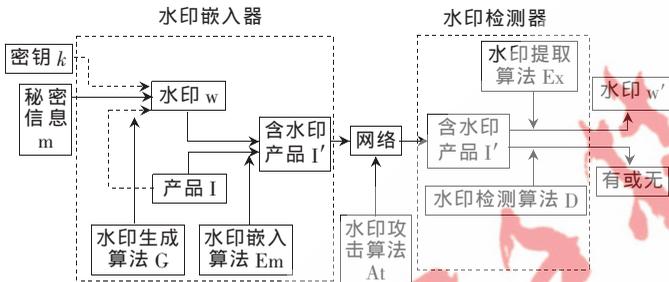


图1 数字水印处理系统基本框架

## 2 数字视频水印理论基础

### 2.1 数字视频水印分类

(1) 按照载体类型可以分为基于压缩视频的水印算法和基于原始视频的水印算法。

(2) 按照水印嵌入域可以分为时空域水印算法和变换域(频域)水印算法。

(3) 按照检测时是否需要原始视频可以分为盲水印和非盲水印。

(4) 按照水印特性可以分为鲁棒水印、脆弱水印与半脆弱水印。

### 2.2 数字视频水印特征

(1) 不可感知性(Imperceptibility)是指用来辨别信号被处理前后的相似性。

(2) 鲁棒性(Robustness)是指作品在遭受了各种信号处理和各种攻击后, 数字水印的可提取性或可检测性。评价数字水印鲁棒性的性能包括脆弱性、有效性和安全性。

(3) 容量(Capacity)是指在单位时间内或在一个数字产品中最多可以嵌入的水印量。

三者之间是相互制约的, 在水印系统中不能同时达到最优性, 只能根据实际需要在三者中进行折中, 其关系如图2所示。

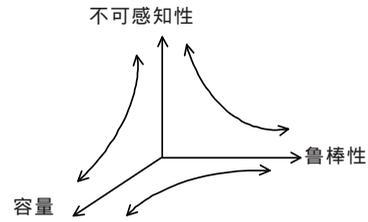


图2 容量、鲁棒性和不可感知性之间的关系

## 3 数字视频水印技术评价

### 3.1 数字视频水印攻击

所谓“攻击”是指对含水印的数字作品执行各种操作, 以此来削弱、移除或破坏水印信息, 其目的是篡改水印信息, 使水印信号检测系统无法提取或检测水印信号。水印攻击的分类如下:

(1) 简单攻击, 又称为波形攻击或噪声攻击。它通过对嵌入水印数据(含水印的作品)的载体进行操作, 以此降低嵌入水印的强度, 导致提取水印信息时发生错误, 甚至无法检测到水印信息。

(2) 同步攻击, 又称为禁止提取攻击。它的目的在于破坏载体数据和水印信息的同步性, 从而使得水印的相关检测失效或无法提取嵌入的水印。

(3) 分析攻击, 也称为计算攻击或去除攻击。在水印的嵌入阶段和检测阶段, 使用特殊的方法来移除或修改载体中的水印, 通过分析水印算法中的数据, 估算载体中的水印信息并分离出水印, 使提取失败, 以达到篡改的目的。

(4) 解释攻击, 又称为IBM水印攻击。当检测到水印信息时, 攻击算法会捏造出很多伪源信息或伪水印信息, 以此来混淆真伪。

### 3.2 数字视频水印性能评估

对水印系统的评价包括主观的评价标准和客观的评价标准<sup>[5]</sup>。主观测试方面, 由于不同的人经历不同, 对水印图像的测试结果差异就会很大, 测试及评估结果不是很有效, 所以在实际的测试中, 往往采用定量的分析方法。

客观测试方面, 常用的标准包括:

(1) 嵌入水印信息量: 当使用同一种水印算法时, 预嵌入的水印量越多, 水印的鲁棒性就越好。

(2) 嵌入水印强度: 预嵌入的水印强度越强, 水印的鲁棒性就越好, 但会增加水印的不可见性。

(3) 宿主信号信息量和特征: 宿主信号信息越大, 特征越明显, 水印系统的鲁棒性就越强。

(4) 密钥信息: 为了防止攻击者采用穷举法破译, 这就需要有足够大的密钥空间(密钥信息值的最大范围), 因此应将密码学原理引入到水印系统中。

一个公平客观的水印性能评估系统, 即使输入的数据测试集不同, 得到的测试结果也应该是相似的。为了在统计上计算结果的有效性, 在测试过程中应采用不用

《微型机与应用》2012年第31卷第7期

## 综述与评论 Review and Comment

的密钥信息和水印信号。通常使用以下评估参数进行测试:

(1) 峰值信噪比 PSNR: 用来衡量嵌入水印的能力, 值越高, 透明性越好。假设:  $I(x, y)$  表示原始图像,  $I'$  表示含水图像,  $M, N$  表示图像尺寸,  $I(i, j)$  表示原始图像中任意一点,  $\max(I)$  表示信号的峰值, 取对数, 可将 PSNR 计算出的值换算成标准单位(即 dB)。公式如下:

$$PSNR = 10 \log_{10} \frac{MN \max[\max(P)]}{\sum_{i=1}^M \sum_{j=1}^N [I(i, j) - I'(i, j)]^2} \quad (6)$$

(2) 相关系数 NC (Normalized Correlation): 用来估算提取的水印图像与原始水印图像之间的相似性, 其中  $W$  表示原始水印图像,  $W'$  表示提取出的水印图像。公式如下:

$$NC = \frac{\sum_{i=1}^M \sum_{j=1}^N I(i, j) I'(i, j)}{\sum_{i=1}^M \sum_{j=1}^N I(i, j)^2} \quad (7)$$

通常在水印系统之间, 很难做到公平的性能评价对比。由于没有统一的评价标准来评测水印系统之间的优劣, 因此水印系统的脆弱性和易攻击性将并存。

### 4 视频水印典型算法

#### 4.1 视频水印算法模型

现有的视频水印算法主要利用扩频通信技术的基本思想, 将视频扩展, 在宿主信号(宽带信道)中传送水印信息(窄带信号)。目前面向视频的的数字水印技术大部分是基于 MPEG 视频压缩的, 因此根据视频编解码的原理, 将 MPEG 视频水印嵌入提取方案分为三种, 如图 3 所示<sup>[6]</sup>。



图3 MPEG视频水印嵌入/提取模型

三种水印嵌入/提取方案及其比较如表1所示。

表1 三种方案的比较

方案描述	方案优点	方案缺点
方案一 水印的嵌入和提取在原始视频码流中进行	水印嵌入方案多, 算法性能好; 可用于数字图像水印方案中	提高视频码流的数据比特速率; 压缩后的MPEG视频质量会降低, 会丢失水印信息
方案二 在视频编码器中执行水印的嵌入和检测	没有增加视频流的数据比特率; 设计出抵抗多种攻击的水印	水印容量小、复杂度较高、会降低视频质量
方案三 水印直接嵌入到压缩的比特流中	计算复杂度低, 不会造成视频质量的下降	水印的数量和嵌入强度小

#### 4.2 基于原始视频的水印算法

原始视频水印是指视频数据不经过压缩, 直接操作, 与视频的扩展名无关。在水印的嵌入和提取的过程中, 根据是否需要变换宿主信号, 将水印细分为空间域

水印和变换域水印。

##### (1) 空间域水印

是指直接将水印信息嵌入到未压缩视频数据的亮度分量或色度分量中, 优点是易于操作且空间复杂度低, 但鲁棒性和不可感知性较差。

Kalker 等<sup>[7]</sup>人提出了一种基于广播通信监控理论的 JAWS (Just Another Watermarking System) 水印算法。该算法的思想是将视频流看作连续的静止图像, 将相同的水印信息嵌入到连续的视频帧中。该算法的缺点是由于水印信息分布不均匀, 因此不利于水印信息的提取, 对于 MPEG-2 视频来说, 鲁棒性差。

Hartung 等<sup>[8]</sup>人提出了一种基于扩频通信技术的空间域水印算法。嵌入水印信息时, 将视频序列看成是空间上的一维信号, 使用扩频通信技术将水印信息变为伪随机序列, 嵌入到原视频序列中, 输出含水水印的视频作品; 提取水印时, 计算伪随机序列和含水水印信息的视频作品之间的相关性。

##### (2) 变换域水印

是指水印的嵌入和提取是在原始视频的某个变换域中进行的, 常用的变换方法包括离散余弦变换 DCT (Discrete Cosine Transform)、离散傅里叶变换 DFT (Discrete Fourier Transform) 和离散小波变换 DWT (Discrete Wavelet Transform)。

Deguillaume<sup>[9]</sup>提出在 DFT 域中, 将视频序列看成是连续、无交叉、固定长度的帧序列, 对于每个帧序列执行相同的水印信息嵌入和提取。

Chen 等<sup>[10]</sup>人提出了一种基于 DCT 域的水印算法: 首先对帧序列进行二维 DCT 变换, 然后提取 DC 系数组成一维矩阵并加密, 再进行一维 DCT 变换, 选择每一小组最后一个高频系数嵌入水印, 令这个系数为  $B'_{j^n}$ , 则  $B'_{j^n} = B_{j^n} + \alpha W_{j^n}$ 。该水印算法抵抗攻击的能力强, 但仅能检测到水印信息, 而不能完整提取水印。

Swanson 等<sup>[11]</sup>人提出一种基于 3-D 小波变换的视频水印算法, 将视频序列看作 3-D 信号, 并将视频序列按场景分类, 可以充分考虑时域的冗余。利用 HVS 掩蔽模型的特性, 确保在每个序列帧中, 水印信息具有鲁棒性和不可感知性。

#### 4.3 基于压缩视频的水印算法

##### (1) 嵌入 DCT 系数

Chung 等<sup>[12]</sup>人将水印信息嵌入到 I 帧的亮度系数中。首先产生一个与 I 帧维数相同、含有整数  $\{-1, 1\}$  的伪随机噪声图案  $W(x, y)$ 。将水印信息调制为扩频水印信号, 并进行适当的缩放, 再将扩频水印信号分成  $8 \times 8$  块, 做 DCT 变换; 然后将压缩视频流中的 I 帧 VLC 进行解码, 得到  $8 \times 8$  块的 DCT 系数, 将每块水印信号的 DCT 直流分量加到与 I 帧亮度相同位置的块 DCT 直流分量上。

## 综述与评论 Review and Comment

Biswass 等<sup>[13]</sup>人将灰度图像水印嵌入到 DCT 系数中, 先对压缩视频流进行部分解码, 采用水印图像分层思想和自适应水印嵌入方式, 提高了算法的鲁棒性和适用性。其嵌入过程如图 4 所示。

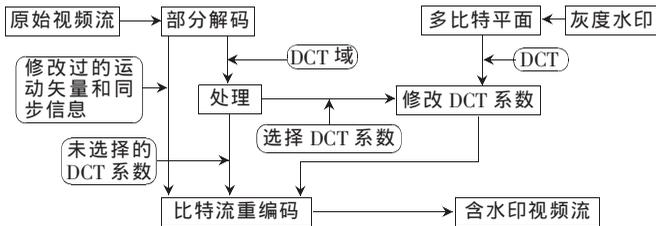


图 4 水印嵌入过程

Noorkami 等<sup>[14]</sup>人利用 H.264 视频压缩标准的特点提出了一种新颖的、复杂性低的 H.264 水印算法, 该方法根据  $4 \times 4$  块的 DC 系数产生公钥, 水印嵌入到量化之后的 AC 系数中, 该系数的选择由版权拥有者的密钥来控制。

### (2) 嵌入运动矢量

Jordan 等<sup>[15]</sup>人提出利用运动矢量进行水印信息嵌入的 MPEG 算法, 此算法通过对运动矢量作微小的修正, 使运动矢量的某个分量的奇偶性与预嵌入的水印信息相联系, 计算复杂度可以忽略, 对于帧比特率的影响也较小。Wang 等<sup>[16]</sup>人提出在 P 帧的运动矢量中嵌入水印, 此算法对视频质量及比特率影响较小, 能减少运动估计的时间。

## 5 人类视觉系统概述

根据人类视觉系统 HAS (Human Visual System) 的特性<sup>[17]</sup>, 一个好的水印算法应该满足不可见性, 嵌入水印后的图像不能引起视觉上的降质。在水印嵌入阶段, 利用人类视觉掩蔽特性, 在满足透明性的条件下, 适当调节数字水印的信息量, 以提高局部嵌入水印信息的强度。人眼对图像信息的分析并不是逐点进行的, 而是对提取空间、频率或色彩特征进行编码。JND (Just Noticeable Difference) 阈值表示数字水印系统所能支持的最大修改值, 使用自适应技术来调节数字水印的嵌入强度, 即使根据人类视觉特性, 也无法分辨出由图像质量产生出来的影响。

目前, 基于人类视觉系统特性的数字水印算法是水印研究的热点。可以将小波变换与人类视觉系统相结合, 通过评估价值来确定鲁棒性, 最大化水印的嵌入量, 提高水印系统的鲁棒性。

## 6 数字水印的应用领域

视频水印主要应用于以下一些领域<sup>[18]</sup>:

(1) 版权保护: 为了识别视频内容的版权, 将由加密技术产生的水印信息嵌入到原始载体中, 并发行含水印的数字视频作品。

(2) 拷贝控制: 当发行数字视频作品时, 使用特殊的机制保护版权。

(3) 内容认证: 为了检测数字视频内容是否被篡改,

可以利用视频水印进行内容认证或完整性校验, 它的特点是认证与内容是相关联的。

(4) 广播监控: 通过数字水印技术可以检测某些视频作品在电视台或广播电台上的播放的时间和次数, 以此保护版权者的所有权。

(5) 盗版追踪: 当视频作品授权给多个用户时, 版权者可将水印信息 (如用户 ID 号) 嵌入到每个数字产品中, 可以避免未经授权的拷贝和发行。

(6) 安全隐蔽通信: 发送方可以将水印信息 (安全信息) 嵌入到视频流中, 接收方根据已知的公钥和密钥来提取水印信息, 而未授权用户是无法提取的, 从而实现了安全传输。

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等问题, 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, 在设计水印算法时, 缺少具有指导性意义的一般框架, 如果能够提出实际可行的具有指导意义的鲁棒性水印模型框架, 将给水印算法设计带来很大的方便。可以预见数字水印用于保护多媒体信息将成为一个越来越流行的热点问题。

### 参考文献

- [1] LEE H Y, KIM H S, LEE H K. Robust image watermarking using local invariant features [J]. Optical Engineering, 2006, 45(3): 037002-037011.
- [2] PITAS I V. The use of watermarks in the protection of digital multimedia products [J]. Proceedings of the IEEE, 1999, 87(7): 1197-1207.
- [3] PODILCHUK C I, DELPE J. Digital watermarking: algorithms and applications [J]. Signal Processing Magazine, 2001, 14(4): 33-46.
- [4] 孙圣和, 陆哲明, 牛夏牧. 数字水印技术和应用 [M]. 北京: 科学出版社, 2004: 45-50.
- [5] HOLLIMAN M, MEMON N. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes [J]. IEEE Transactions on image processing, 2000, 9(3): 432-441.
- [6] 施鹏飞, 赵立初. 数字水印技术的研究 [J]. 信息与控制, 2000(2): 40-45.
- [7] KALKER T, DEPOVERE G, HAITSMAN J. A video watermarking system for broadcast monitoring [C]. Proceeding of SPIE on Security and Watermarking of Multimedia Contents, San Jose, 1999: 103-112.
- [8] HARTUNG F, GIROD B. Watermarking of uncompressed and compressed video [J]. Signal Processing, Special Issue on Copyright Protection and Access Control for Multimedia Services, 1998, 66(3): 283-301.
- [9] DEGUILLAUME F, CSURKA G, RUANAIDH J. Robust 3D

- DFT domain video watermarking [C]. Proceeding of SPIE on Security and Watermarking of Multimedia Contents. San Jose, 1999:113-124.
- [10] CHEN T H, LIU S H, YAO H X, et al. Robust video watermarking based on DC coefficients of selected blocks [C]. Proceeding of the Fourth Int conference on Machine Learning and Cybernetics, Guangzhou, 2005:5273-5278.
- [11] SWANSON M, ZHU B, TEWFIK A. Multi-resolution Scene-based Video Watermarking Using Perceptual Models [J]. IEEE Journal on Selected Areas in communications, 1998,16(4):540-550.
- [12] CHUNG T Y, HONG M S, SHIN DH, et al. Digital watermarking for copyright protection of MPEG-2 compressed video [J]. IEEE Transactions on Consumer Electronics, 1998,44(3):895-901.
- [13] BISWAS S, DAS S R, PETRIU E M. An adaptive compressed MPEG-2 video watermarking scheme [J]. IEEE Transactions on Instrumentation and Measurement,2005,54(5):1853-1861.
- [14] NOORKAMI M, MERSEREAU R M. Compressed-domain video watermarking for H. 264 [C]. Proceeding of IEEE International Conference on Image Processing, Genoa, 2005:890-893.
- [15] JORDAN F, KUTTER M, EBRAHIMI T. Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video[C]. MPEG-4 Meeting, Technical Report M2281, ISO/IEC Document,Stockholm, 1997:125-130.
- [16] WANG P, ZHENG Z D, YING J. A novel video Watermark technique in motion vectors [C]. Proceeding of IEEE International Conference on Audio Language and Image Processing. Shanghai, 2008:1555-1559.
- [17] DELAIGLE J F, DEVLEESCHOUWER C. Human visual system features enabling watermarking [C]. Proceeding of ICME 2002, Multimedia and Expo,2002:489-492.
- [18] DOERR G, DUGELAY J L. A guide tour of video watermarking [J].Signal Processing:Image Communication, 2003,18:263-282.

(收稿日期:2011-11-08)

## 作者简介:

刘敏,男,1974年生,高级讲师,主要研究方向:计算机教学。