半脆弱数字水印技术在 MPEG 中的应用*

王 磊, 王道宪, 段晓辉
(北京大学电子学系, 北京 100871)

摘 要: 在 MPEG-2 标准视频编解码协议的基础上, 将静态图像水印的一些算法移植到视频水印中, 做到了既可以抵抗数字产品在传输过程中的失真、一些常见的图像/视频处理过程, 同时又可以检测到一些恶意的攻击、篡改等。同时提出了一套针对 MPEG 视频协议的半脆弱数字水印认证算法。

关键词: 半脆弱数字水印; MPEG; 多媒体认证; Gray 编码
中图分类号: TP309 文献标识码: A 文章编号: 0529-6579 (2004) S2-0169-04

1 原理和算法

该多媒体认证算法是一种盲检测的算法。发送方从原始的图像中提取有意义的信号作为水印信号嵌入到图像中去。在接收方, 当收到嵌入水印的图像以后, 用私钥解开水印信号, 通过对比通过图像提取的信号与嵌入的水印信号, 达到版权认证的目的[1-6]。

1.1 水印信号的提取

(1) 将 DCT 变换后的 DC 系数作为宏块的特征值加以利用。

假设经过分块后, 得到了 n 个不相重叠的块, 每块中提取了 k bit 的信息。矢量 $B_i(1*k)$ 被定义为第 i 块的信息。首先计算每一个块 A_i 的均值然后找到这些值中的最大值与最小值。量化系数 Δ 定义如下: $\Delta=\dfrac{\max(A_i)-\min(A_i)}{2^k}$, 而 B_i 等于:

$$B_i=\begin{cases}00 & \text{if } \min<A_i<\min+\Delta\\ 01 & \text{if } \min+\Delta<A_i<\min+2\Delta\\ 11 & \text{if } \min+2\Delta<A_i<\max-\Delta\\ 10 & \text{if } \max-\Delta<A_i<\max\end{cases}$$

由此可见, 当 k 越大的时候, 量化系数 Δ 越小, 结果也越精确。在本文中, $k=4$。

这里已经采用 Gray 码对量化系数进行了编码。

(2) 对量化完的水印信号做 ECC 编码。

由于 $k=4$, 编码方式从 0000-1111, 可以利用 BCH (7, 4, 1) 码。刚好可以纠正一位的错误。至此, 得到了水印信号的生成方式。流程如图 1 所示。

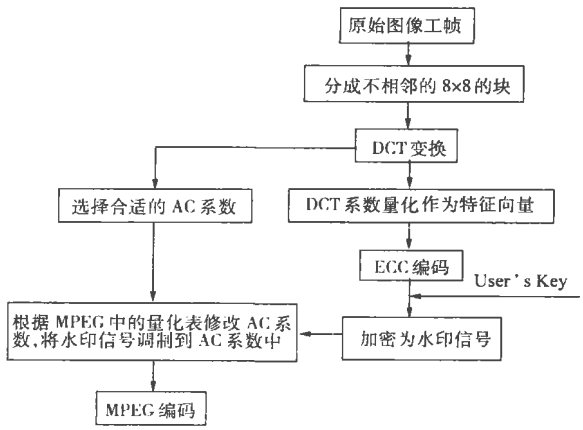

图 1 水印嵌入算法流程

Fig. 1 The flow chart of the watermark imbedding arithmetic

1.2 水印信号的嵌入

我们将水印信号嵌入到 DCT 系数中图像的低频部分。在提取的信号 S 被嵌入之前我们用了私钥对其加密, 得到水印信号 M: M=Sx or Key。在这里我们直接用密码做异或运算, 解码的时候只要再做一次异或运算即可。然后对选择的 DCT 系数 $W(x, y)$ 进行量化。

水印嵌入规则如下: 若水印信号 $M(i)=0$, 而该位系数是量化系数的偶数倍, 则不改变该位系数; 反之 $W(x, y)=W(x, y)+Q$。若水印信号 $M(i)=1$, 而该位系数是量化系数的奇数倍, 则不改变该位系数; 反之 $W(x, y)=W(x, y)+Q$。

1.3 水印信号的认证

接收者可以从视频流中提取出水印信号, 算法由图 2 给出。

第 1 步, 将图像分割成为不相邻的块, 对 DC

* 收稿日期: 2004-09-11
作者简介: 王 磊 (1981 年生), 男, 硕士研究生; E-mail: Wanglei@ele.pku.edu.cn

系数进行统计分析。重构水印信号。第 2 步，对每一块 DCT 变换后的 AC 系数反量化，计算其与量化系数的比值，提取水印信号。第 3 步，利用 ECC 纠错码的解码方式纠正传输过程中的噪声，或者一些基本的图像处理造成的误码。第 4 步，利用密钥从水印信号中恢复每一块的信息。第 5 步，将提取的水印信息与从 DC 系数提取的图像特征值做比较，以进行认证。

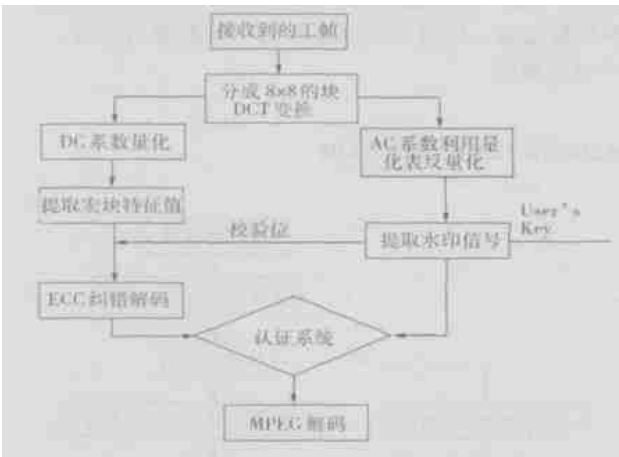

图 2 水印认证算法流程

Fig. 2 The flow chart of the watermark authentication arithmetic

2 实验结果和结论

2.1 水印信号对 I 帧质量的影响

选择了 PSNR、PSNR 分散度两方面衡量算法对图像质量的影响（图 3）。从视觉效果上来说，两者没有什么区别。下面研究一下 PSNR 与 PSNR 分散度的情况。

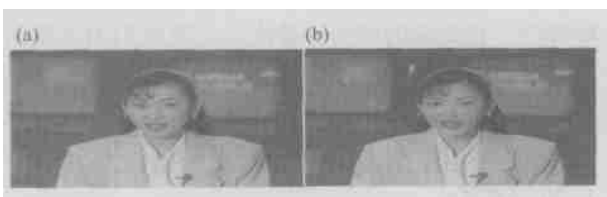

图 3 原始 I 帧(a)与嵌入水印后的 I 帧(b)对比

Fig. 3 The comparison between the aboriginal I frameand the embedded one

图 4 给出了 3 幅图像（I 帧）的 PSNR 曲线图。很明显，随着量化阶数 Q 的升高，图像的质量在下降。而且 I 帧的 PSNR 下降不是很快，基本能够满足视觉上的要求。按照 TASO 提出的图像质量评分和峰值信噪比的关系 [极好（感觉不到干扰）48；良好（刚刚感觉到干扰）35；可接受（明显感到干扰，但不令人讨厌）29；临界状态（干扰令人讨厌）25]，水印信号对 I 帧质量的影响是在良好以上。下表给出了 PSNR 分散度的值，从中我们可以发现，I 帧嵌入水印后带来的误差是均匀分布的，这跟我们将水印均匀嵌入到图像的各个块中是相吻合的。

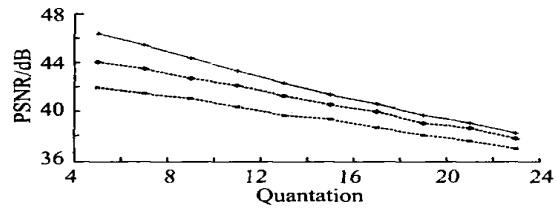

图 4 I 帧的 PSNR 曲线图

Fig. 4 The PSNR graph of the I frame

I 帧	Akiyou	Mobile	Coastgard
PSNR 分散度	672	588	614

2.2 水印信号对攻击的检测

就目前水印技术的发展，对以下几类常见的水印攻击分别分析如下：

2.2.1 噪声攻击（gauss noise attack） 采用研究的最多、最成熟的高斯噪声模型。

因为：Watermark ∝E(image)；而高斯噪声均值为 0，即：

$$E(\text{image}) = E(\text{image} + \text{Gauss}) =$$
$$E(\text{image}) + E(\text{Gauss}) = E(\text{image}) + 0$$

因此高斯噪声对宏块的特征量没有影响。在嵌入水印的时候高斯噪声影响的是 DCT 系数的高频段，所以对水印认证没有影响。

2.2.2 低通滤波（low pass gilter） 典型的例子是低通平滑滤波。

明显的，通过平均模板处理后的 I 帧，灰度部分会发生变化且是连续性变化。因此，对特征值做了 ECC 纠错编码以后，就可以抵御低通滤波处理。同样的，一些类似的滤波处理也可以得到相似的结论。实验结果证明，低通滤波后的 I 帧是可以通过水印认证系统的。

2.2.3 替换攻击 将原始视频中的某些部分或者某些信息做了修改，或者将原始视频中一些版权保护的标记（如电视台的台标等）替换成其他的版权标记。如图 5 所示。

对于这样的替换，由于替换者不知道加密算法的密钥，因此无法准确的复制出水印信号。并且可以根据水印信号被破坏的程度和位置定位出黑客篡改的区域。

2.2.4 几何攻击 对于图像水印，最著名的基准工具是 Unzign 和 Stirmark，整合了一系列不同的几

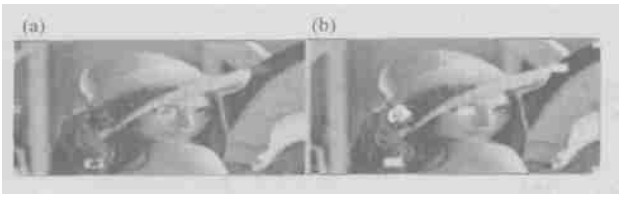

图 5　替换攻击与检测结果
(白色方块为认证确定的被篡改区域)
Fig. 5　The replacing attack

何攻击。此类攻击多见于对图像中的某些感兴趣区域的修改 (注意不是替换)。一般鲁棒水印通过较为复杂的同步运算，是可以抵御这类攻击的。但我们将此类攻击视为恶意攻击 (篡改)。在本算法中没有引入同步信息的概念，因此对此类攻击是敏感的。图 6 将女主角的领子部位做了几何变换，图 6 (b) 则是水印检测的结果。

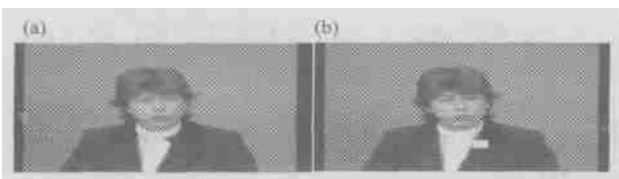

图 6　几何攻击的检测
Fig. 6　The geometrical attack

2.2.5　*基于估计的攻击*　攻击者在没有嵌入规则或者全部嵌入秘钥的知识的情况下，通过估计原始信息或者水印通过利用一些比如最大相似度的准则，进行攻击。但我们的水印校验模型是按 bit 进行校验，只要有 1 bit 的错误就不能通过验证系统。因此这类攻击无效 (图 7)。

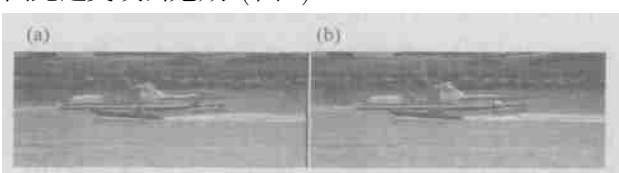

图 7　基于估计的攻击
Fig. 7　The estimation based attack

在该画面中，攻击者通过对水印的估计，将船标修改，水印算法同样检测到这样的攻击方式并且准确的定位出来。

2.2.6　*基于统计的攻击*　这种攻击是基于对水印信号嵌入的规则进行大量的统计。从而破解加密算法的密钥。本文中的算法由于采用的是最简单的加密处理，故在这方面有不足。进一步的改进可以利用一些基于 MD－5 等具有较强加密性能的密钥算法。

综上所述，半脆弱水印的适用范围：高斯噪声、低通滤波、替换攻击、几何变换、估计攻击、统计攻击的敏感程度分别为不敏感、不敏感、敏感、敏感、敏感、敏感。

3　总　结

本篇针对 MPEG 2 编码的视频流提出一种半脆弱水印的嵌入算法，以达到既能抵抗常规的视频传输中的图像处理，又能检测到恶意攻击以实现版权认证的目的。其特点在于：在水印信号的提取上，充分利用了 MPEG 本身的一些特性，简化了复杂度，而且取得较好的效果；对水印信号的编码，采用了 Gray 码和 ECC 编码，有效地实现了对正常图像处理的包含和对恶意攻击的检测；对水印信号的嵌入，嵌入方式完全可以由 MPEG 本身的量化表来完成，故最大限度的利用了 MPEG 算法本身对图像质量的影响获得最大限度的嵌入水印能量；同时根据密码学的知识引入了对水印信号的加密算法，提高了安全性。

参考文献：

[1]　毕厚杰. 多媒体信息的传输与处理[M]. 北京：人民邮电出版社, 1999.

[2]　冯登国. 国内外信息安全研究现状及发展趋势[J]. 世界科技研究与发展, 2000, 22(2)：2－8.

[3]　魏为民. 基于彩色静止数字图像的信息隐藏技术研究[J], 数据采集与处理, 2002, 17: 84－89.

[4]　KUNDUR D. Multi resolution digital watermarking: Algorithms and implications for multimedia signals dissertation[D]. Department of Electrical and Computer Engineering, University of Toronto, 1999.

[5]　MEER P W. Digital image watermarking in the wavelet transform domain[D]. Salzburg: University of Salzburg, 2001.

[6]　LIN C Y, CHANG S F. Semi-fragile watermark for authenticating JPEG Visual content[J]. Washington, SPIE, 2000: 140－151.

(下转第 175 页)

[5] CHIOU G H, CHEN W T. Secure broadcasting using the secure lock[J]. IEEE Transaction on Software Engineering, 1989, 15(8): 929—934.

Hierarchical Access Control for Secure Group Communication

SU Ming, LIU Gang
(Department of Computing Science the Information and Engineering University, Zhengzhou 450002, China)

Abstract: Secure group communication with hierarchical access control refers to a scenario where a group of members is divided into a number of subgroups located at different privilege levels and a high-level subgroup can receive and decrypt massages within any of its descendant lower-level subgroups; but the converse is not allowed. To propose a improved scheme, which is based on the Chinese Remainder Theorem. The scheme not only enables secure hierarchical control but also provides the following properties: hiding of hierarchy and receivers, authentication of both senders and messages, and a mechanism for the receiver to directly derive the key of a message.

Key words: secure group communication; hierarchical access control

---

(上接第 171 页)

The Application of Semi-fragile Digital Watermark Technology in the MPEG

WANG Lei, WANG Dao-xian, DUAN Xiao-hui
(Department of Electronics, Peking University, Beijing 100871, China)

Abstract: Based on the MPEG-2 video coding standard, some watermark arithmetics used in static image process are introduced to the video watermarking. And the goal is achieved that not tampering with the video quality at the same time of according with the MPEG-2 coding standard, and being tolerant of the transmission distortion and normal image/video processes as well as detecting some intended attacks and sophistication. In addition a digital watermark authentication arithmetic aimed at the MPEG standard is proposed.

Key words: semi-fragile watermark; MPEG; video authentication; gray coding