

# 基于矩阵置乱的自适应视频水印算法

刘稚洁 刘延申

(华中师范大学教育信息化研究中心, 武汉 430079)

**摘要** 视频数字水印技术是当前水印研究中的一个热点。为了更好的保证视频水印的鲁棒性,提出了一种基于MPEG-2运动分量的自适应数字水印算法。该算法首先利用矩阵置乱来确定水印片段的目标图像组,然后结合人眼视觉系统选择水印比特嵌入的运动分量。实验结果表明,该算法不仅对于针对视频水印的特殊攻击具有高鲁棒性,且水印嵌入前后图像的峰值信噪比仅有微弱差异。

**关键词** 视频水印 运动分量 矩阵置乱 图像组

中图分类号: TP391 文献标识码: A 文章编号: 1006-8961(2005)11-1471-05

## Adaptive Video Watermarking Algorithm Based on Matrix Scrambling

LIU Zhi-jie, LIU Yan-shen

(Educational Informatization Research Central, HuaZhong China Centre Normal University, Wuhan 430079)

**Abstract** Digital watermarking technology of video image is a hot topic in present watermarking researching area. In this paper, a adaptive video watermarking scheme based on MPEG-2 motion vectors is proposed, using matrix scrambling computing target group of pictures for watermark clip, combined human visual system, choosing target component motion for watermarks bit. Experimental show that it is robust to special video watermarks attack, and has faintness influence on the visual effect of pictures.

**Keywords** video watermarking, component motion, matrix scrambling, group of pictures

## 1 引言

随着计算机和多媒体网络技术的发展,数字媒体的传输与获取变得日益便捷,但同时也导致数字产品成为非法侵权、盗版行为的对象。数字水印技术<sup>[1]</sup>作为解决该问题的一个重要方法,已经从图像领域发展到音频、视频和文本等领域。由于大量数字视频产品,如VCD(video compact disc)、DVD(digital video disc)的出现,使得对视频数字产品版权保护的市场需求日益迫切,因而视频数字水印技术也成为当前水印研究中的一个热点<sup>[2,3]</sup>。

视频数字水印技术是通过向视频序列中隐藏版权信息来达到保护视频版权的目的。与静止图像水印相比,视频水印除了要满足前者的要求外,还有自身的特殊要求:首先,必须实现盲检测,即在水印提

取过程中,不需要原始视频的参与;同时,视频水印算法必须简单、快捷,能满足实时性。另外,一些针对视频水印的特殊攻击方式的出现,对鲁棒性也提出新的要求。这些专门针对视频水印的攻击方式主要包括帧替换、帧重组、帧添加、帧删除等,它们的攻击形式如图1所示。

由于目前市场上的视频多采用MPEG格式压缩后,再进行保存和传输,所以视频水印算法还必须与压缩算法兼容。为了保证这一点,可以采用在压缩域嵌入水印,即对压缩后的视频数据流嵌入水印。在压缩域水印算法方面,Hartung等提出的基于DCT(discrete cosine transform)系数的视频水印技术是目前研究得最多的技术<sup>[4,5]</sup>,但是其算法复杂,且会对视频解码系统中的运动补偿环路造成不良影响;而另一种压缩域水印算法——运动矢量算法,由于它具有计算复杂度极小,且充分利用了视频水印的

收稿日期:2005-08-15; 改回日期:2005-09-10

第一作者简介:刘稚洁(1983~),女,2004年毕业于中国地质大学(北京),现为华中师范大学硕士研究生。主要研究方向为数字水印、视频处理。E-mail: gfordaisy@yahoo.com.cn

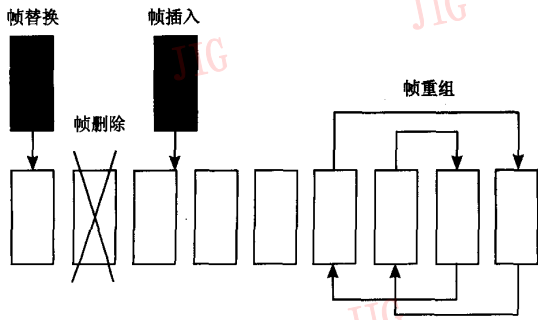


图 1 针对视频水印的特殊攻击

Fig. 1 Special attack on video watermark

动态性等优点,已经日益成为人们关注的研究课题。Kutter 等第 1 次提出了运动矢量水印算法<sup>[6]</sup>。它是通过修改运动矢量的奇偶性来嵌入水印。Zhang 等改进了嵌入规则,选择幅值较大的运动矢量,同时根据运动矢量的相位角情况采取不同的嵌入方法<sup>[7]</sup>。戴侃斐等提出结合 MPEG-4 编码规则,只修改运动矢量的标志位,使压缩过程中选择了不同的运动补偿方式<sup>[8]</sup>。以上这些算法均具有实现简单,对视觉效果影响小等优点,但是没有考虑到对帧删除等视频水印特殊攻击的鲁棒性。

本文中提出了一种首先将水印分成多个片段,并运用生命游戏矩阵置乱算法在 MPEG-2 压缩域确定各水印片段的目标图像组,然后对该图像组的所有帧进行嵌入操作,同时结合人眼视觉特性自适应地在每一帧中选择水印嵌入运动分量的算法。这种算法可通过生命游戏的单向性来保证嵌入水印的安全性,而且对视频水印特殊攻击具有较强的鲁棒性。

## 2 基于生命游戏的矩阵置乱算法

### 2.1 生命游戏介绍

生命游戏是一类特殊的图像矩阵变换<sup>[9]</sup>,它具有不可逆性,其在地理学、经济学、计算机科学等领域都有非常广泛的应用。它的具体规则如下:

把一个  $j \times j$  二值矩阵想象成是由上下、左右边界相接而构成的封闭空间,其每一个位置都可以看成是一个细胞,且每个细胞都有生和死两种状态。如果某位置的值为 1,则表示该位置的细胞为生,反之为 0,则为死。每个细胞的生死由它的 8 个邻居细胞确定,其所遵循的原则为:对某个细胞而言,如果邻居有 3 个是活的,则不管它之前是什么状态,都

变成活的;如果邻居有两个是活的,则它保持原状态不变;除此之外,一律让它死去。

根据以上规则,矩阵内的杂乱无序细胞就构成了一个复杂的动态世界,而且会逐渐演化出多种精致结构。

### 2.2 矩阵置乱算法

设需要置乱的矩阵为  $E$ ,其大小是  $r \times r$ 。置乱时,首先生成一个伪随机序列  $J$ ,并按扫描线顺序将其头尾相接填入大小为  $r \times r$  的 2 维矩阵  $F$ ;然后将  $F$  作为细胞的初始状态矩阵,并对其进行多步生命游戏迭代,再根据其每一步迭代结果对  $E$  进行置乱,最后把置乱结果存储在预先建立的一个大小为  $r \times r$  的空矩阵  $G$  中。

假设  $T_0$  表示细胞的初始状态矩阵, $T_i$  表示进行完第  $i$  步生命置乱得到的结果矩阵,矩阵  $T_i = \bigcup_{0 \leq k \leq i} T_k$  表示经过  $i$  步生命置乱,所有存活过的细胞集合矩阵。令  $T^{(i)} = \hat{T}_i - \hat{T}_{i-1}$ ,表示从来没有存活过的细胞中经过第  $i$  次生命游戏活过来来的细胞集合矩阵。具体置换步骤如下:

(1) 令  $T_0 = F$ ,按照光栅顺序读取  $T_0$  中,值是 1 的位置在  $E$  中所对应的值,并将这些值按光栅顺序依次填入空矩阵  $G$  中;

(2) 对  $T_0$  进行  $z$  步生命游戏迭代,每次迭代后根据矩阵  $T^{(i)}$ ,将需要置乱的矩阵  $E$  中的值填入空矩阵  $G$  的后续空位;

(3) 若在某一次迭代过程中  $G$  被填满,则终止迭代。如果在  $z$  步迭代完成后, $G$  仍未被填满,则令  $T^{(z)}$  为  $\hat{T}_z$  的取反,表示在这  $z$  步生命游戏中从来没有存活的细胞集合矩阵,再根据取反后的  $T^{(z)}$  对  $G$  进行填充即完成置乱。其中迭代步数  $z$  需要结合  $r$  的情况选取。

## 3 基于生命游戏的水印算法

MPEG-2 视频序列的第 1 层是图像序列层,它包含序列头、若干个图像组的数据以及序列终止符。图像组 (GOP, group of picture) 作为随机操作单元,由定义的一组或多组帧内编码帧 (I 帧) 或非帧内编码帧 (P 帧或 B 帧) 图像组成。每组包括组头和图像层数据,组头中 group-start-code 参数表示图像组的起始。视频压缩时,可对一个图像组内的帧从 1 开始编号,一直到最后一帧。本方法将充分利用图

像组的概念,把其作为水印片段的嵌入和提取的单位,使 group-start-code 参数成为水印提取的定位锚,以保证视频水印面对特殊攻击时的鲁棒性。具体的实现步骤如下:

#### (1) 水印生成

假设需要嵌入的水印为一幅二值图像  $I_w$ , 大小是  $M_w \times N_w$ 。首先产生伪随机水印序列  $K_w$ , 并把它按扫描线顺序首尾相接地填入大小为  $M_w \times N_w$  的掩码矩阵  $Y_w$  中; 同时, 将  $I_w$  与  $Y_w$  进行异或, 即得到加密后的水印图像  $\hat{I}_w$ ; 然后将  $\hat{I}_w$  分成大小为  $\hat{M}_w \times \hat{N}_w$  的  $m$  块, 如果在边界处像素不够, 则以 0 补充; 接着将这些块编号为  $\hat{I}_w[k]$  ( $0 < k \leq m$ )。  $m, \hat{M}_w, \hat{N}_w$  的选择可根据实际情况确定, 但需要满足几个条件:  $\hat{M}_w \times \hat{N}_w$  需小于一帧中所包含的宏块的数量, 且  $m$  小于整个视频序列中 GOP 的数量; 最后要将每个块分别按照扫描线顺序转化成 1 维二值序列。

#### (2) 根据矩阵置乱求水印片段的目标图像组

求目标图像组时, 首先从视频序列中选择  $n \times n$  个图像组,  $n = \lceil lbm \rceil$ , 将这些图像组的编号从小到大填入大小为  $n \times n$  矩阵  $E$ ; 然后生成一个伪随机矩阵  $K_1$ , 根据由  $K_1$  生成的矩阵  $F$  对  $E$  进行置乱; 最后将置乱结果矩阵  $G$  按照光栅顺序转化为 1 维数组  $H$ 。此时,  $H[k]$  的值即为与  $\hat{I}_w[k]$  对应的目标图像组的编号。

#### (3) 水印嵌入

本论文使用的是在运动矢量上嵌入水印的方法。运动矢量表示每个宏块相对于预测块位移的情况, 每个运动矢量由水平方向和竖直方向两个运动分量组成。根据人眼视觉系统对快速运动物体的敏感性不如对慢速运动物体的敏感性高, 而快速运动的部分一般在某个方向上有较大的运动分量的特点, 若在具有较大绝对值的运动分量上添加水印则会降低水印的可见性。具体嵌入算法如下:

首先对需要嵌入水印的帧进行解码, 并查看所有运动矢量的水平分量和竖直分量, 然后选取其中绝对值最大的  $\hat{M}_w \times \hat{N}_w$  个运动分量, 最后在其上嵌入水印。

设  $S$  是需要嵌入的水印比特, 当需要将其嵌入到运动分量  $P$  上, 则所采用的嵌入法如下:

若  $P \geq 0$ , 则

$$\hat{P} = \begin{cases} P + \gamma, & \text{mod}((P \times q + D), 2) \neq S \\ P, & \text{mod}((P \times q + D), 2) = S \end{cases}$$

若  $P < 0$ , 则

$$\hat{P} = \begin{cases} P - \gamma, & \text{mod}((P \times q + D), 2) \neq S \\ P, & \text{mod}((P \times q + D), 2) = S \end{cases}$$

其中,  $\hat{P}$  为嵌入水印后的运动分量;  $D = 2L$ ,  $L$  为运动估计搜索窗口的长度;  $\gamma = (2n + 1)/q$ ,  $q$  用于控制嵌入强度,  $n$  为一整数。嵌入时, 之所以分  $P \geq 0$  和  $P < 0$  两种情况考虑, 是为了保证水印嵌入使运动分量的绝对值增大, 且不影响提取阶段目标运动分量的选择。

#### (4) 水印检测

水印检测工作是嵌入算法的逆运算, 且满足盲检测条件。水印检测时, 首先根据  $K_1$  计算每个水印片段的目标图像组, 然后从目标图像组的每个帧中选取绝对值最大的  $\hat{M}_w \times \hat{N}_w$  个运动分量, 依次从每个分量上提取出水印比特, 提取公式为:

$$\hat{S} = \text{mod}((P \times q + D), 2)$$

接着根据从目标图像组各预测帧中提取出来的比特序列, 按照投票规则来确定水印片段的每一位; 最后将各个水印片段拼合起来, 用  $K_w$  解码, 即得出原始水印图像。

## 4 实验

### 4.1 对视觉效果的影响

本文采用画面运动比较显著的 Table tennis、运动比较平缓的 Susie 和包含较多细节信息的 Flower garden 这 3 个 MPEG-2 标准视频序列进行试验, 视频参数见表 1。

表 1 视频参数

Tab. 1 Video parameters

参数	视频名称		
	Flower garden	Susie	Table tennis
图像大小	352 × 240	704 × 480	352 × 240
码率 (bit/s)	2M	8M	1M
帧速率 (帧/s)	30	30	25
GOP 帧数	15	15	15
I/P 距离	3	3	3
总帧数	450	450	375

水印图像是一幅  $184 \times 160$  的二值图像, 嵌入时将其分成 8 块, 即需要 8 个 GOP 来嵌入水印。图 2、图 3 分别显示未嵌入水印的视频图像和嵌入水印后



(a) Susie

(b) Flower garden

(c) Table tennis

图 2 未加水印的视频图像

Fig. 2 Video images without watermarks



(a) Susie

(b) Flower garden

(c) Table tennis

图 3 嵌入水印后的视频图像

Fig. 3 Video image with watermarks

的视频图像试验结果。

从图 2、图 3 可以看出,水印嵌入后重建的视频图像与原始视频图像从主观视觉上看,两者几乎没有差异,可满足不可感知要求。表 2 显示了水印嵌入前后视频序列的平均峰值信噪比 (peak signal noise ratio, PSNR) 和二者的差值以及 WDR (watermarks detected ratio)。由表 2 可以看出,水印的嵌入对重建图像的峰值信噪比影响很小,基本上不影响图像的显示质量。

表 2 水印嵌入前后的平均峰值信噪比与水印正确检测率

Tab. 2 Comparison of average peak signal to noise ratio before and after embedded and watermarks detected ratio

	Flower garden	Susie	Table tennis
$\overline{PSNR}_0$ (dB)	40.536 1	35.757 1	38.970 9
$\overline{PSNR}_1$ (dB)	40.652 4	35.833 4	38.966 3
$\delta$	0.116 3	0.076 3	0.004 6
WDR	1.0	1.0	1.0

#### 4.2 嵌入算法的安全性分析

无论是图像水印,还是视频水印都有安全性方

面的要求,即水印被嵌入后,只要不知道确定的参数,即使知道水印算法也不能从嵌入水印的视频中将水印移除。由于基于生命游戏的置乱方法具有不可逆性,因此要移除水印,攻击者必须选择置乱密钥。如果采用穷举破解,则需要对所有的帧都进行水印提取工作,且需将提取出来的水印与水印图像的每个块进行比较。假设一个视频序列含有 50 帧,水印图像被分成了 8 块,那么比较次数的期望最少也将达到  $8^{50}$ ,这在时间上是一个无法接受的指标。根据以上的分析,可知采用生命游戏进行目标图像组的选择,对于解释攻击有强健的鲁棒性。

#### 4.3 面对特殊攻击时的鲁棒性的实验

实验采取的攻击方法是从每个图像组中选择几帧进行置换、删除、重组。因为在进行删除攻击时,从一个 GOP 中提取出的正确水印序列数总是占多数,所以采取该算法总可以提取出正确的水印。由于重组操作一般是图像组内进行的,因此对水印提取效果没有影响。

图 4 展示了进行置换攻击时,正确提取出的比特百分比随着受攻击帧率变化的曲线,图中横坐标为受攻击帧率,纵坐标为水印正确检测概率 (WDR)。

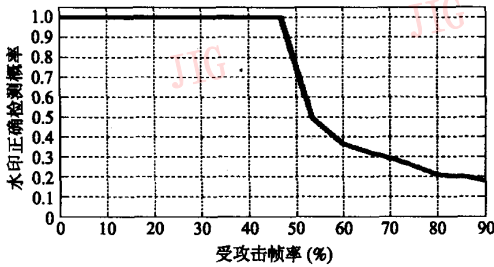


图 4 稳健性—置换特殊攻击强度曲线

Fig. 4 Robust—replacement intensity curve

由图 4 可以看出,受攻击帧率小于 50% 时,总可以提取出正确的水印图像。

## 5 结 论

本文提出了一种基于运动矢量的视频数字水印算法,该算法的特点在于先利用生命游戏置乱来选择各水印片段的目标图像组,然后根据人类视觉模型自适应地选择目标运动分量。该方案对解释攻击和针对视频水印的特殊攻击具有很强的鲁棒性。同时该算法具有实现简单、视频质量下降微弱、可与 MPEG-2 压缩标准紧密结合等优点。

### 参考文献 (References)

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

2 Eggers J J, Girod B. Blind watermarking applied to image authentication [A]. In: Proceedings of International Conference on Acoustics, Speech, and Signal Processing 01 [C], Salt Lake City, Utah, USA, IEEE Computer Press, 2001: 1 ~ 4.

3 Swanson M D, Tewfik A H. Multimedia data embedding and watermarking technologies [J]. Proceedings of the IEEE, 1998, 86(6): 1064 ~ 1087.

4 Hartung F, Girod B. Watermarking of uncompressed and compressed video [J]. Signal Processing, 1998, 6(3): 283 ~ 301.

5 Christoph B, Wolfgang F, Stephen W. Digital watermarking: From concepts to real-time video application [J]. IEEE Computer Graphics and Applications, 1999, 19(1): 25 ~ 35.

6 Jordan F, Kutter M, Ebrahimi T. Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video [A]. In: MPEG4 Meeting, Technical Report M2281, ISO/IEC Document, JTCL/SC29/WG-11, Stockholm, Sweden, 1997.

7 ZHANG Jun, LI Jie-gu, ZHANG Ling. Video watermark technique in motion vector [A]. In: 2001 proceedings of XIV Brazilian Symposium on Computer Graphics and Image Processing [C], Florianópolis, Brazil, 2001: 179 ~ 182.

8 DAI Kan-fei, HUANG Wen-yong, CHEN Zhen-yong, et al. An MPEG4 vector watermarking scheme based on scrambling using game of life [J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2004, 43(11): 192 ~ 195. [戴佩斐, 黄文勇, 陈真勇等. 基于生命置乱的 MPEG-4 运动矢量水印算法 [J]. 中山大学学报 (自然科学版), 2004, 43(11): 192 ~ 195.]

9 Berlekamp E, Conway J, Guy R. Winning ways for your mathematical plays [M]. New York, USA: Academic Press, 1982.