

基于生命游戏置乱的 MPEG-4 运动矢量水印算法^{*}

戴侃斐, 黄文勇, 陈真勇, 唐 龙

(清华大学计算机科学与技术系, 北京 100084)

摘 要: 提出一种基于 MPEG-4 视频对象运动矢量的视频水印算法, 它直接对压缩后的视频数据流进行操作, 将经过置乱的水印信息嵌入到运动矢量的标志位上, 与视频压缩标准有很好的兼容性。实验结果表明, 该算法简洁有效, 嵌入水印所引起的信噪比的损失很小。此外, 算法采用具有单向特性的生命游戏置乱来抵抗解释攻击。

关键词: MPEG-4; 运动矢量; 视频水印; 生命游戏; 置乱

中图分类号: TP391 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0192-04

随着计算机和多媒体网络技术的发展, 数字媒体的获取与传输变得非常简单, 但同时也导致了数字产品的盗版和侵权行为, 版权保护已成为信息安全的重要课题。数字水印^[1]技术是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。视频数字水印技术是当前水印研究中的一个热点, 主要原因是随着大量数字视频产品如 VCD、DVD 的出现, 对视频数字产品版权保护的**市场需求日益迫切。

大多数视频水印算法主要是在图像水印算法上进行的改进, 这些算法虽简单, 但鲁棒性不高。而视频与图像最重要的区别在于它在时间上是动态的, 因此, 在动态区域上进行水印嵌入, 也就是运动矢量水印算法, 已经成为人们关注的研究课题。将水印信息嵌入到运动矢量中, 能更加有效地利用视频信息。Kutter 等^[2]第一次提出了运动矢量水印算法, 通过修改矢量分量的奇偶性来嵌入水印。Zhang 等^[3]改进了嵌入规则, 选择幅值较大的运动矢量。此类方法实现简单, 但运动矢量的奇偶性易被改变, 算法的鲁棒性较差。Bodo 等^[4]在对运动矢量进行分等级的分析后, 划分出大小为 $N \times N$ 的运动矢量等级, 再将水印分布在较低等级的矢量中。此方法鲁棒性有所提高, 但计算复杂度太大, 编码效率太低。

上述这些算法都是针对基于矩形帧的运动矢量, 而新一代多媒体数据压缩编码标准 MPEG-4 是一种基于对象的高效压缩算法^[5], 在运动估计和运动补偿上采用了 H. 263 中的半像素搜索技术。本

文提出一种基于生命游戏置乱的 MPEG-4 运动矢量水印算法, 通过生命游戏的单向性来抵制“二次水印”的解释攻击, 并且修改所选取运动矢量的类别以增强鲁棒性, 算法简洁, 且几乎不影响编码效率和视频质量。

1 基于生命游戏的置乱算法

1.1 生命游戏介绍

生命游戏是一类特殊的图像矩阵变换⁶。英国数学家 John Conway 和他的学生在 1970 年前后, 确定了生命游戏并给出了恰当的规则。

假设平面网格上, 每个网格代表一个生命细胞, 给网格涂黑色代表此细胞为活, 涂白色代表此细胞为死。如果平面网格无限大 (事实上, 可以把有限网格上下、左右边界相接), 那么每个网格有 8 个邻居。这 8 个细胞的状态将对它们所包围的细胞状态产生影响。对给定的网格初始状态, 应用如下规则处理:

(1) 若周围相邻网格恰好有 3 个为黑色, 则该网格应修改为黑色;

(2) 若周围相邻网格恰好有 2 个为黑色, 则该网格保持原状态不变;

(3) 此外, 无论此网格原始状态如何, 该网格都要修改为白色。

1.2 基于生命游戏的图像置乱算法

假设集合 Z 表示平面网格内所有细胞都是成活的状态, 即平面网格上所有网格的集合。假设集合 S_0 表示给定的平面网格的初始状态, 即初始状

* 收稿日期: 2004-09-11

基金项目: 国家自然科学基金会重点项目研究计划资助项目 (60133020)

作者简介: 戴侃斐 (1980 年生), 女, 硕士研究生; E-mail: dlf02@mails.tsinghua.edu.cn

态下成活细胞的集合； S_i 表示迭代到第 i 步时成活细胞的集合， $i > 0$ 。 $S^{(i)} = \bigcup_{0 \leq j \leq i} S_j$ 表示迭代到第 i 步时所有成活过的细胞的集合。则基于生命游戏的置乱算法可以如下定义：

- (1) 建立平面网格与数字图像上像素点的一一映射；
- (2) 对于平面网格的初始状态 S_0 ，将成活细胞对应的像素点按扫描线顺序排列在置乱图像坐标空间内；
- (3) 迭代到第 i 步时，将 $S^{(i)} - S^{(i-1)}$ 中的细胞对应的像素点按扫描线顺序排列在置乱图像坐标空间内；
- (4) 若迭代到第 N 步时终止，则将 $Z - S^{(N)}$ 中的细胞对应的像素点按扫描线顺序排列在置乱图像坐标空间内。

2 基于置乱的 MPEG-4 运动矢量水印算法

生命游戏的规则简单，但是具备非常好的单向特性。水印算法使用生命游戏置乱算法产生水印嵌入位置，由于生命游戏的单向性，在不知水印的前提下，攻击者无法获知水印的嵌入位置，这就大大加强了水印的鲁棒性。算法包括初始化、生成初始图像、确定嵌入位置、水印嵌入和水印检测 5 个主要步骤。

2.1 初始化

初始化的过程包括三部分：
(1) 对水印图像进行置乱并分割，得到每一帧中的待嵌入水印。

假设待嵌入的水印图像为 $M_w \times N_w$ 的二值图像 I_w ，首先对水印图像进行置乱：

- ①随机产生一个密钥 K_w ，将 K_w 进行二进制编码后按扫描线顺序首尾相接的填入到大小为 $M_w \times N_w$ 的矩阵 S_w 中；
- ②将 S_w 作为初始状态，迭代次数取值为 $M_w \times N_w$ ，对水印图像进行生命游戏置乱，得到置乱后的水印图像 I_w' 。
- ③将 I_w' 依次分割成大小为 $M_w \times N_w$ 的块 $I_w[i]$ ，最后一块若不够则以 0 补齐，然后将 $I_w[i]$ 作为每一帧中要嵌入的水印。其中， $i = 1, 2, \dots, [(M_w \times N_w) / (M_w \times N_w)]$ 。

- (2) 选择备选运动矢量。
对于每一个待嵌入水印的 P 帧或 B 帧，随机选择 $2M_w \times 2N_w$ 个运动矢量，作为备选运动矢量，将它们的位置放入备选矩阵 $E[i]$ ($i = 1, 2, \dots$ ，

$[(M_w \times N_w) / (M_w \times N_w)]$) 中，这里所选运动矢量的宏块是在 VO 的内部或者边界上，并且选择的运动矢量的幅度应尽可能大，这样有助于提高鲁棒性^[3]。

- (3) 生成掩码矩阵。

随机产生密钥 K_w ，将 K_w 进行二进制编码后按扫描线顺序首尾相接的填入到大小为 $M_w \times N_w$ 的掩码矩阵 Y_w 中。

2.2 生成初始图像

对于每一待嵌入水印的 P 帧或 B 帧，用下列方法来生成初始图像 $S_0[i]$ ：

- ①设 $S_0[i]$ 为一大大小为 $2M_w \times 2N_w$ 的 $\{0, 1\}$ 矩阵，用 1 代表细胞为活，0 代表细胞为死。初始时各位置上都为 0。
- ②将水印 $I_w[i]$ 与掩码矩阵 $Y_w[i]$ 进行按位异或运算，将结果放入到 $S_0[i]$ 的左上角，即 $M_w \times N_w$ 的位置。
- ③再将水印 $I_w[i]$ 与掩码矩阵 $Y_w[i]$ 进行按位异或运算再按位取反，将结果放入到 $S_0[i]$ 的右下角。
- ④按扫描线顺序，将 $S_0[i]$ 循环右移 $K_w \bmod (2M_w \times 2N_w)$ 次。

2.3 确定嵌入位置

按前面描述的基于生命游戏的置乱方法，对 $S_0[i]$ 进行迭代处理。其中迭代次数 N 的取值为 $M_w \times N_w$ 。将由置乱方法生成的最后 $M_w \times N_w$ 个点在运动矢量域上所对应的原始位置作为水印的嵌入位置。

2.4 水印嵌入

MPEG-4 采用了 H.263 的半像素搜索 (half pixel searching) 技术。运动矢量的搜索算法分为两步。第一步是以宏块中亮度信号块 ($16H \times 16V$) 为基准，在预先确定的搜索区域内进行全搜索，得到一个像素精度的运动向量。第二步是以第一步运动估计的整数位移点为中心，对周围的 8 个半像素点 (由周围整像素点抽样值内插得到) 区域进行搜索。这 8 个半像素点位置分别为 $(0.5, \pm 0.5)$ ， $(\pm 0.5, 0.5)$ ， $(0, \pm 0.5)$ 和 $(\pm 0.5, 0)$ 。两步搜索匹配的准则均为最小绝对帧差平均 (MAE)。

视频编码时它们将分为 3 类： 16×16 块匹配的搜索结果 MV_0 ； 16×8 块匹配的搜索结果 MV_{5-8} ，即位置 $(0, \pm 0.5)$ 和 $(\pm 0.5, 0)$ ； 8×8 块匹配的搜索结果 MV_{1-4} ，即位置 $(0.5, \pm 0.5)$ ， $(\pm 0.5, 0.5)$ 。选择 MAE 值最小的搜索结果作为最终选择的运动矢量，并且设置相应的标志，如表 1 所示。

表 1 MPEG-4 运动矢量类别与相应的标志设置

Tab 1 Types and symbol settings of MPEG-4 motion vectors

选中类别	Has4MVForward 标志	FieldMV 标志
16× 16	FALSE	FALSE
16× 8	FALSE	TRUE
8× 8	TRUE	无影响

我们的水印算法通过修改选择的运动矢量类别将水印矩阵 $I_w [i]$ 嵌入到当前的 B 帧或 P 帧中:

(1) 当 $I_w [i] [j] = 0$ 时, 采用第 1 类的运动矢量。

(2) 当 $I_w [i] [j] = 1$ 时, 采用第 3 类的运动矢量。同时, 强制使得块编码选择标志 Skip 为 FALSE。因为, 当 Skip 为 TRUE 时, MPEG 4 编解码器将会根据运动矢量的值的大小 (比如, 全 0 的情况), 将 Has4MVForward 标志重设为 FALSE, 默认为直接编码模式。其中, $j = 0, 1, \cdots, M_w \times N_w$ 。

相比以往的算法, 本算法并不直接修改运动矢量的值, 而是改变被选择的运动矢量类别, 由于 3 类运动矢量都是搜索出来的结果, 用它们来进行运动补偿, 效果差别事实上不大, 对编码效率几乎没有影响; 同时, 不必考虑运动矢量的模的大小, 只要不是在 VO 外部的宏块, 都有运动矢量, 都可用来嵌入水印。

2.5 水印检测

据所知的两个密钥和水印图像, 可知道置乱后的水印图像与每一帧中水印的嵌入位置。然后检测该位置的宏块的 Has4MVForward 标志来提取水印。当所有帧中的水印都提取出来以后, 将它们拼接, 得到 I_w' , 再进行逆置乱, 即可提取出水印图像 I_w 。

3 实验结果

我们分别以运动较为显著的 Foreman 视频, 运动不是很明显的 Akiyo 视频, 以及有两个视频对象的 News 视频进行实验。视频格式为 CIF (352×288)。初始水印图像如图 1, 大小为 94×29。每一帧中嵌入 25 个水印分量, 这样共需要 $[94 \times 29 / 25] = 110$ 帧来嵌入水印。水印嵌入前后的视频对象如图 2 所示, 取第四帧为例。提取出的水印图像如图 3。实验结果表明, 水印能正确地提取出来。实验性能如表 2 所示, 分别取视频流的第 4 帧, 第 50 帧的 Y 亮度信号为例。

Tsinghua

图 1 原始水印图像
Fig. 1 Original watermark

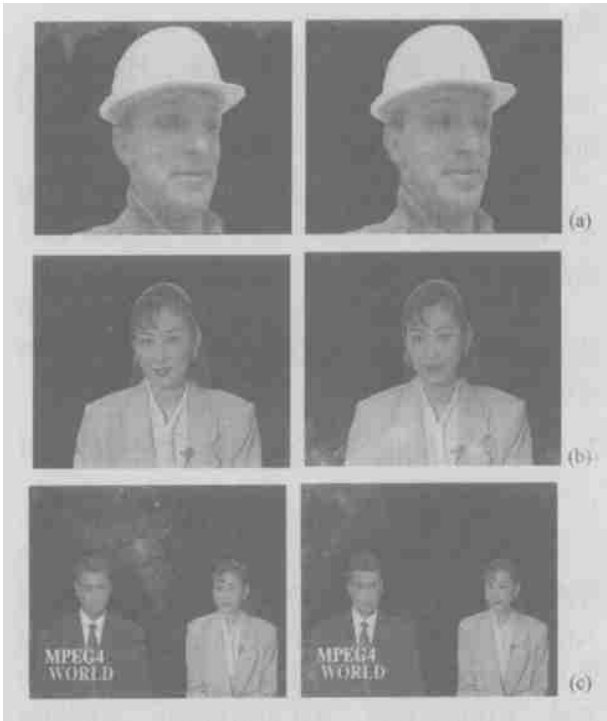


图 2 嵌入水印前后的视频
Fig 2 Original and watermarked frames from three sequences
(a) Foreman; (b) Akiyo; (c) News



图 3 从视频中提取的水印图像
Fig 3 Extracted watermarks from three sequences
(a) Foreman; (b) Akiyo; (c) News

表 2 实验性能
Tab 2 Experimental results

视频名称	未嵌入水印视频 PSNR/dB		嵌入水印视频 PSNR/dB		水印检测错误位数
	第 4 贴	第 50 贴	第 4 贴	第 50 贴	
Foreman	39.90	38.85	39.88	38.84	1
Akiyo	39.87	39.87	38.57	38.57	0
News	39.04	38.62	39.04	38.61	0

从表 2 可以看出, 由于水印算法只是修改了运动矢量的标志位, 对矢量本身的大小没有改变, 水印嵌入后, 基本上不影响视频的质量。而且, 可嵌入水印的数目与视频运动矢量的模的大小也没有关系, 相反, 对于运动不太明显的 Akiyo 和 News 视

频, 水印造成的影响几乎可以忽略。

4 结 语

本文提出了一种基于生命游戏置乱和 MPEG-4 运动矢量的水印新算法。算法有两个明显的优点:

首先, 给出了运动矢量水印研究的一个新思路, 水印没有修改运动矢量的实际值, 而只是修改了运动矢量的标志位, 使其选择了不同的运动补偿方式, 因此, 水印的嵌入并没有降低视频的质量, 有效利用了视频本身的信息。其次, 利用了生命游戏的单向性, 抵抗对水印的解释攻击。

解释攻击并不以图像中已经存在的水印本身为攻击目标, 而是设计出一种情况使得原水印所标识信息的可靠性受到置疑。这种攻击的典型情况即是“二次水印”。其本质思想是: 由于很多数字图像水印方案并没有提供本质的方法来检测两个水印中哪一个是先加上去的。因此, 存在这样的情况: 图像 I 的所有者对图像嵌入了水印 W , 而生成嵌入水印后的图像 $D = I + W$, 并将 D 发布了出去; 攻击者可以借此用自己的水印 W^* 构造新的图像 $D^* = D - W^*$, 并声称对 D 拥有所有权, 且原始未标记的版本为 $D^* = D - W^*$ 。在这种情况下, 图像 I 所有者的原有水印 W 的可靠性就受到了质疑。这个问题是由 Craver 等^[7] 在 1998 年提出的, 并引出了单向水印方案的概念。

水印方案的非可逆性对于阻止解释攻击是必要的。如果攻击者对加密图像进行“二次水印”等解释攻击, 由于基于生命游戏的置乱方法所具有的单向性, 那么他将面临的一个难题就是如何选择合适的水印以及密钥, 使得产生的结果是可以被识别的。也就是, 攻击者必须要使得新加入的水印同时

满足有意义和具备真实性这两个特征。但是由于生命游戏的单向性, 攻击者没有直接的办法由加密图像生成去掉指定水印的伪造原始图像。如采用穷举法破解, 由于水印长度至少为 100 位, 每一位上与加密图像对应位置上含义相符的概率为 0.5, 则攻击者要尝试的次数的期望值至少为 2^{99} 次; 并且水印长度每增加一位, 攻击者需要尝试的次数就要增加一倍。这是一个时间上不可接受的策略, 因此该水印嵌入方案可以有效的抵抗“二次水印”的攻击。

参考文献:

- [1] VOYATZIS G, PITAS I. The use of watermarking in the protection of digital multimedia products [J]. Proceeding of IEEE, 1999, 87(7): 1197—1207
- [2] JORDAN F, KUTTER M, EBRAHIMI T. Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video [C]. ISO/IEC M2281, 1997.
- [3] ZHANG J, LI J, ZHANG L. Video watermark technique in Motion vector [J]. Computer Graphics and Image Processing, 2001: 179—182.
- [4] BODO Y, LAURENT N, DUGELAY J. Watermarking video, hierarchical embedding in motion vectors [J]. ICIP03. 2003, 2: 739—742.
- [5] EBRAHIMI T, HORNE C. MPEG-4 natural video coding——an overview [J]. Signal Processing, 2000, 15(4—5): 365—385.
- [6] BERLEKAMP E, CONWAY J, GUY R. Winning ways for Your mathematical plays [M]. Academic Press, 1982.
- [7] CRAVER S, MEMON N, YEO B. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications [J]. IEEE Selected Areas in Communications, 1998, 16(4): 573—586.

An MPEG-4 Motion Vector Watermarking Scheme Based on Scrambling Using Game of Life

DAI Kan fei, HUANG Wen yong, CHEN Zhen yong, TANG Long

(Department of Computer Sciences and Technology, Tsinghua University, Beijing 100084, China)

Abstract: A video watermarking scheme for the motion vector of MPEG-4 video object is proposed. Via operating the compressed video data stream directly, the permuted watermark is embedded into the motion vector indicators. Therefore, the scheme has a good compatibility with the compression standard. Experimental results show that the proposed algorithm is considerable simple and efficient, and PSNRs of watermarked frames are reduced rather slightly. In addition, the scheme employs the noninvertible life-game scrambling to resist the protocol attacks.

Key words: MPEG-4; motion vector; video watermarking; game of life; scrambling