

文章编号:1001-9081(2011)06-1508-04

doi:10.3724/SP.J.1087.2011.01508

基于压缩传感的视频水印算法

周 燕,曾凡智

(佛山科学技术学院 计算机系,广东 佛山 528000)

(zhouyan791266@163.com)

摘要:针对压缩域视频流的完整性认证问题,提出了一种基于压缩传感(CS)的视频水印算法。以H.264压缩视频流为研究对象,通过对视频序列的I帧进行压缩传感随机投影,得到少量的测量值,经过量化和置换加密,最后以水印的方式嵌入到P帧具有最大运动矢量幅值的宏块中。认证时,从含水印视频序列的P帧提取水印,并对I帧进行相同的压缩传感随机投影,通过比较测量值的差异,实现对视频的完整性认证。仿真结果表明,该算法具有较好的视频质量,对码率的影响较小,对帧删除、帧插入、重压缩等攻击具有较强的鲁棒性。

关键词:H.264;视频水印;压缩传感;随机投影;视频认证

中图分类号:TP391.41;TP309 **文献标志码:**A

Video watermarking algorithm based on compressive sensing

ZHOU Yan, ZENG Fan-zhi

(Department of Computer Science, Foshan University, Foshan Guangdong 528000, China)

Abstract: For the problem of integrity authentication about compressed video streams, this paper proposed a video watermarking algorithm based on Compressive Sensing (CS). The H.264 compressed video stream was taken as the research object. By conducting random projection on the I frames of video sequences, a slight amount of measurements were obtained. Through quantization and replacement encryption, the measurements were embedded into the macro block which had the maximum amplitude in the motion vector in P frame. While authenticating, the watermark was extracted from the P frame that contains watermarked video sequences, and the similarly random CS projection on the I frames was conducted. By comparing the difference between the measurements, the integrity of video could be authenticated. The simulation results show that the intended video watermarking algorithm ensures high video quality, and little effect on the encoding rate, and it has strong robustness against attacks such as frame deletion and frame insertion.

Key words: H.264; video watermarking; Compressive Sensing (CS); random projection; video authentication

0 引言

随着视频的应用发展,视频安全是一个值得重视的问题。数字水印技术作为保护视频安全的一种有效手段,已在版权保护、视频完整认证、数字指纹等多个领域有所应用^[1-5]。视频水印算法主要分为两类:基于原始视频的水印算法和基于压缩视频的水印算法。对基于原始视频的水印算法:1)由于嵌入水印后的视频数据在有损压缩时可能丢失部分水印信息;2)对于已压缩的视频,需要先解码,嵌入水印后再重新编码,将增加计算的复杂性并降低视频的质量。因此目前的研究重点是基于压缩域的视频水印。

基于压缩域的视频水印算法是将水印信息嵌入到编码后的视频流中,主要包括在I帧的离散余弦变换(Discrete Cosine Transform, DCT)系数和在P、B帧的运动矢量中嵌入水印^[6-9]。H.264作为新一代视频编码标准,具有很高的压缩率,而水印是利用载体的冗余空间进行操作的,压缩性能越好,冗余空间就越小,因此水印嵌入越困难。王美华等人^[10]提出在H.264视频编码时,根据I帧DCT低频量化系数关系生成认证码,然后以水印的形式把认证码嵌入到I帧DCT高频量化系数中。由于只在DCT高频交流系数AC₁₁~AC₁₅位

置上嵌入水印,因此该算法的载体容量比较低,且对B、P帧的攻击行为会出现漏检。Profrock等人^[11]提出利用I帧的哈希函数值作为认证码,嵌入到P、B帧的Skip宏块中。由于哈希值的计算复杂度大且耗时,以及哈希函数的不可逆性,使得该算法没有定位能力。

针对目前的压缩域视频水印算法存在的问题,本文提出一种基于压缩传感(Compressive Sensing, CS)的视频水印算法。由压缩传感理论可知^[12],在一定条件下,通过少量的测量值就可以准确重构出原始信号,也就是说少数的测量值能够保持原始信号的结构和足够多信息。利用该特性,通过对H.264视频序列的I帧进行压缩传感随机投影^[13],得到能够代表I帧图像特征的少量测量值,经过量化和置乱加密,以水印的方式嵌入到P帧中具有最大运动矢量幅值的宏块中。由于测量值数目较少,因此嵌入的水印信息相对较少,水印嵌入对视频质量和码率的影响较小,算法对帧删除、帧插入等攻击具有较强的鲁棒性。

1 基于压缩传感的视频水印框架

本文提出的基于压缩传感的视频水印框架如图1所示。压缩传感是在稀疏表示和优化理论的基础上提出的一种

收稿日期:2010-11-22;修回日期:2011-01-22。

基金项目:广东省自然科学基金资助项目(1015280001000016;1045280001004185)。

作者简介:周燕(1979-),女,江西抚州人,讲师,硕士,主要研究方向:图像处理、智能信息;曾凡智(1964-),男,湖北武汉人,副教授,博士,主要研究方向:数据挖掘、图像处理。

数据采样理论,其本质是对信号进行随机投影,以低于Nyquist的采样率得到少量观测值,然后通过求解一系列优化问题,得到原始信号的逼近。随机投影是一个从高维到低维的变换过程。设信号 $\mathbf{x} \in \mathbb{R}^N$ 在变换域 Ψ 上可以表示为:

$$\mathbf{x} = \Psi \mathbf{s} = \sum_{i=1}^N \Psi_i s_i \quad (1)$$

其中: $\mathbf{s} = [s_1, \dots, s_N]$ 是 N 个权值系数 $s_i = \langle \mathbf{x}, \Psi_i \rangle$ 构成的 N 维权值向量, $\Psi = [\Psi_1 | \Psi_2 | \dots | \Psi_N]$ 是 $N \times N$ 维的变换矩阵, Ψ_i 是其第 i 个列向量。

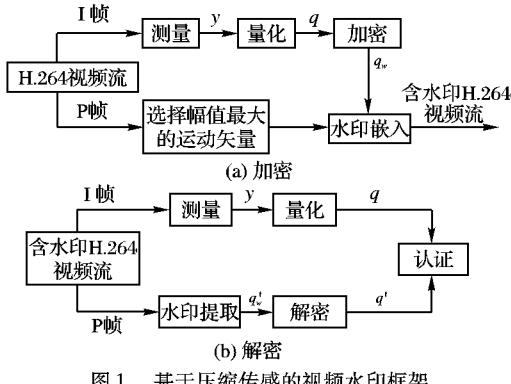


图1 基于压缩传感的视频水印框架

向量 \mathbf{x} 在变换域 Ψ 上 K 稀疏表示 \mathbf{s} 的 N 个系数中有 K 个非零项,且 $K \leq N$ 。压缩传感直接采样信号的 M ($K < M \leq N$) 个随机测量值,即:

$$\mathbf{y} = \Phi \mathbf{x} = \Phi \Psi \mathbf{s} \quad (2)$$

其中: Φ 表示 $M \times N$ 的测量矩阵, \mathbf{y} 表示长度为 M 的测量向量。

2 水印生成与嵌入

H.264 标准将每个视频图像分成 16×16 的像素宏块,使得视频图像能以像素宏块为单位进行处理。一个 I 帧图像通常划分成若干宏块,一个宏块由一个 16×16 亮度像素和附加的一个 8×8 Cb 和一个 8×8 Cr 彩色像素块组成。设 I 帧图像的大小为 N ,第 i 个像素宏块的向量形式记为 \mathbf{x}_i ,其中 $i = 1, \dots, n$ ($n = N/16^2$)。

2.1 随机投影

在压缩传感的随机投影中,测量矩阵需要满足约束等距性(Restricted Isometry Property, RIP)条件^[14],目前所采用的测量矩阵大多为非确定性测量矩阵,即随机矩阵。本文采用稀疏随机测量矩阵,矩阵的构造方式如下:

- 1) 首先生成一个零元素的矩阵 $\Phi \in zeros^{M \times N}$, $M < N$ 。
- 2) 在矩阵 Φ 的每一个列向量中,随机地选取 d 个位置, $d \in \{4, 8, 10, 16\}$ 。
- 3) 把所选取位置的值赋为 1。

相对应像素宏块的分块方式,把 Φ 分成 $M_{16} \times 16^2$ 的矩阵块 Φ_{16} ,其中 $M_{16} = \lfloor (M \times 16^2)/N \rfloor$,即矩阵 Φ 用块对角矩阵表示:

$$\Phi = \text{diag}[\Phi_{16}, \Phi_{16}, \dots, \Phi_{16}] \quad (3)$$

对每个像素宏块 \mathbf{x}_i 采用相同的矩阵块 Φ_{16} 进行投影测量,得到测量向量:

$$\mathbf{y}_i = \Phi_{16} \mathbf{x}_i \quad (4)$$

2.2 量化加密

对测量向量 \mathbf{y}_i 进行量化,设量化步长为 Δ ,输入为 $\mathbf{y} = (\mathbf{y}_i)$,输出为 $\mathbf{q} = (q_i)$ 。量化方程如下:

$$(\Delta u)_i = \mathbf{y}_i - q_i; i = 1, 2, \dots \quad (5)$$

其中: \mathbf{y}_i 为测量向量, q_i 为量化规则。 q_i 由式(6)确定:

$$q_i = \arg \min_{a \in A} \left| \sum_{j=1}^r (-1)^{j-1} \begin{bmatrix} r \\ j \end{bmatrix} u_{i-j} + \mathbf{y}_i - a \right| \quad (6)$$

其中: $|u_i| \leq 2^{-1}\delta$,并且 $|\mathbf{y}_i - q_i| \leq 2^{-1}\delta$ 。

量化后的测量值 \mathbf{q} 在作为水印嵌入前,先对其进行加密处理,以提高水印的安全性。本文采用置换加密,方法如下:

$$q_w = E(\mathbf{q}, K) \quad (7)$$

其中: E 为加密算法, K 为置换密钥, \mathbf{q} 为测量值, q_w 为加密后的水印。根据置换密钥的定义,置换密钥的空间大小为 $n!$,即数组 $\{0, 1, 2, \dots, n\}$ 的全排列。由于加密后的测量值重新排序,攻击者获得正确置换密钥的概率为 $1/n!$,提高了水印的安全性。

2.3 水印嵌入

在运动矢量中嵌入水印是通过修改运动矢量的奇偶性来实现的。在视频序列中,变化较快的部分具有较大的运动矢量,而人眼视觉系统对快速运动物体的敏感性低于慢速运动物体,因此修改幅值大的运动矢量对视频质量的影响较小。本文通过把水印嵌入到 P 帧中具有最大运动矢量幅值的宏块中,水印嵌入宏块的选择算法如下:

- 1) 选择 P 帧中采用帧间预测编码的宏块作为水印嵌入的候选宏块;
- 2) 计算每一候选宏块的运动矢量的幅值,找出具有最大运动矢量幅值的宏块;
- 3) 通过修改运动矢量的奇偶性来嵌入水印。

以水平分量为例,运动矢量的修改规则如下:

$$V'_i = \begin{cases} V_i + 1, \text{mod}(\text{abs}(V_i), 2) \neq q_i, & \text{且 } V_i > 0 \\ V_i - 1, \text{mod}(\text{abs}(V_i), 2) \neq q_i, & \text{且 } V_i < 0 \\ V_i, \text{mod}(\text{abs}(V_i), 2) = q_i \end{cases} \quad (8)$$

其中: V_i 为运动矢量的水平分量, q_i 为待嵌入的水印信息, V'_i 为嵌入水印后得到的运动矢量的水平分量, mod 为取模运算, abs 为取绝对值运算。

如果一个宏块中嵌入了水印信息,与其相邻的宏块则不再添加水印。对于运动矢量的垂直分量,可以采用相似的嵌入方法。

2.4 误差补偿

由于 P 帧中的运动矢量采用差值编码方式,如果改变了某一个运动矢量的分量值,紧跟其后的运动矢量的对应分量也会改变,从而造成误差累积。水印嵌入引入的误差累积不仅会降低图像质量,而且嵌入水印后的运动矢量的平均值很可能因此而改变。通过误差补偿可以解决这个问题,补偿方法是若嵌入水印对运动矢量做了加(减)1 操作,则对需要补偿的块运动估计搜索得到的运动矢量的值减(加)1。

3 水印提取与认证

水印提取是水印嵌入的逆过程。从 P 帧中已嵌入水印的运动矢量宏块中提取水印,得到加密的水印 q'_w ,然后对水印进行解密,得到量化值 q' 。

认证时,采用水印生成的方法,对含水印的 H.264 视频流的 I 帧进行随机投影,测量值经过量化,得到量化值 q 。然后与

运动矢量中提取出来的量化值 q' 进行按位异或运算, 最后按式(9)计算不为零的位所占比率:

$$p = \frac{1}{m} \sum_{i=0}^m b_i \quad (9)$$

其中: m 为水印的比特数, b_i 为异或运算后不为零的位。设置一个阈值 τ 来决定认证是否通过, 如果 $p < \tau$, 表示认证通过, 否则认证不通过。

4 仿真实验

采用 H.264 编码标准的参考软件 JM8.6 实现本文的视频水印算法, 实验所使用的视频序列以及参数如表 1 所示。本文主要从水印对视频质量和码率的影响以及水印的鲁棒性等方面进行仿真实验。

表 1 测试视频序列及参数

视频序列	I 帧周期	I/P 间隔	帧率	帧的大小
Suzie	12	3	25	176 × 144
Carphone	12	3	30	352 × 240
Tennis	12	3	25	352 × 288

4.1 水印对视频质量的影响

在低码率的 H.264 视频压缩时, 一个画面组 (Group of Pictures, GOP) 内 P 帧和 B 帧所占的比例较大, 且采用了可变分块大小运动估计, 因此具有更多的运动矢量。如果视频流中的 I 帧图像足够稀疏, 根据理论推算, I 帧图像经过压缩传感随机投影得到的测量值数量 M 约为图像大小 (176×144) 的 1% (约为 250), 因此嵌入到 P 帧的水印相对较少, 保证了水印嵌入后视频的质量。图 2 是 Suzie 视频序列第 17 帧 (P 帧) 嵌入水印前后的实验结果对比, 从图中可以看出, 水印嵌入后, 仍能保持较好的视觉效果, 满足不可感知条件。



图 2 Suzie 序列水印嵌入对比

为了客观评价水印对视频质量的影响, 采用峰值信噪比 (Peak Signal-to-Noise Ratio, PSNR) 来比较嵌入水印前后的视频质量。通过实验, 上述 3 组视频序列第 17 帧 (P 帧) 嵌入水印前后的 PSNR 如表 2 所示。从表中可以看出, 嵌入水印后, P 帧图像的信噪比下降幅度很小, PSNR 的变化都在 0.2 dB 以内, 说明本文算法透明度较好。

表 2 视频序列嵌入水印前后的 PSNR 对比 dB

视频序列	PSNR	
	原始	嵌入水印后
Suzie	38.92	38.75
Carphone	40.21	40.08
Tennis	41.09	40.98

4.2 水印对码率的影响

在视频序列中嵌入水印, 对视频码率有一定的影响。对于 P 帧, 嵌入水印后码率会略有增加。表 3 为 Suzie 序列的 P 帧嵌入水印前后码率的变化, 从表中可以看出, 平均增加的码率低于 1%, 因此水印算法是有效的。

表 3 Suzie 序列嵌入水印前后码率变化 bps

状态	P 帧	平均码率
水印嵌入前	128 492	103 650
水印嵌入后	129 004	104 330

4.3 水印的鲁棒性

通过一系列的外加视频干扰来检测算法的鲁棒性, 包括帧删除、帧插入、重压缩等。算法鲁棒性是通过比较提取的水印与原始嵌入的水印的相关性来判定, 这里采用归一化相关函数来表示提取水印与原始水印的相似程度:

$$N_c = \sum_{i=0}^{M-1} q_{wi} q'_{wi} / \sum_{i=0}^{M-1} (q_{wi})^2 \quad (10)$$

其中: q_w 和 q'_w 分别表示原始水印和提取的水印, M 表示水印的长度。

在码率为 1 Mbps 的情况下, 提取水印与嵌入水印的 $N_c = 0.986$ 。对含水印的视频重新压缩, 在不同压缩率下的 N_c 值如表 4 所示。随着压缩率的提高, 正确提取的原始水印逐渐减少。从绝对值看, 低码率下 N_c 值仍较高。从实验结果来看, 码率在 0.9 Mbps (原压缩率的 90%) 以上的情况下, 提取的水印与原始水印的相似度较高。

表 4 视频序列在不同压缩率下的 N_c 值

视频序列	码率/Mbps				
	1.00	0.95	0.90	0.85	0.80
Suzie	0.986	0.937	0.902	0.879	0.865
Carphone	0.978	0.928	0.889	0.871	0.859
Tennis	0.982	0.932	0.897	0.874	0.867

对嵌入水印的 Suzie 视频序列进行帧删除和帧插入的攻击, 然后比较提取的水印与原始水印的 N_c 值, 并与文献 [10] 的算法进行对比。帧删除的实验结果如图 3 所示, 帧插入的实验结果如图 4 所示。从图 4 中可以看出, 随着删除帧数和插入帧数的增加, N_c 值逐渐降低, 但都保持在 0.9 以上, 表明水印具有较强的抗攻击能力。在相同的删除帧数和插入帧数的情况下, 本文算法得到的 N_c 值也略高于文献 [10] 的算法得到的 N_c 值。

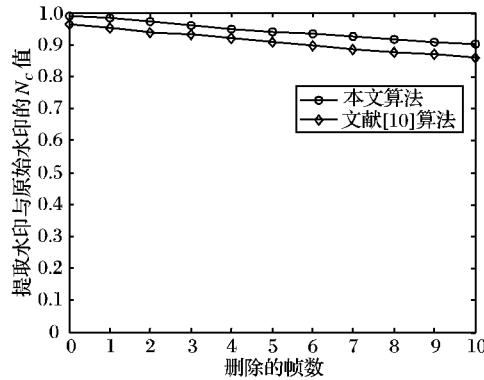


图 3 帧删除的水印鲁棒性分析对比

5 结语

由压缩传感的特性出发, 把压缩传感引入到视频水印中, 提出了一种基于压缩传感的视频水印算法。仿真结果表明, 算法具有较小的码率变化和较好的视频质量, 并且对帧删除、帧插入等攻击具有较强的鲁棒性。由于 I 帧 DCT 系数之间

能量关系比较稳定,适合嵌入鲁棒性水印,而P、B帧适合在运动矢量中嵌入脆弱水印,下一步研究在I帧中嵌入版权认证水印,然后对含水印的I帧图像进行压缩传感随机投影,最后把水印信息嵌入到P、B帧的运动矢量中,从而实现版权认证和内容认证。

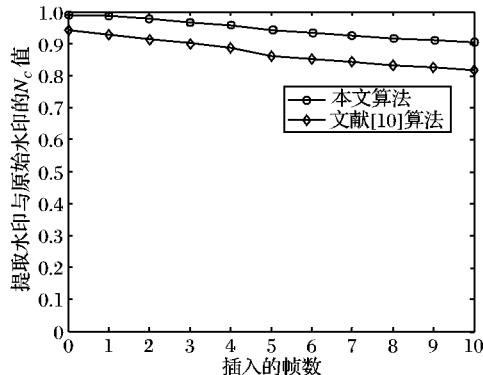


图4 帧插入的水印鲁棒性分析对比

参考文献:

- [1] 李智,陈孝威.基于熵模型的高透明性自适应视频水印算法[J].软件学报,2010,21(7):1692-1703.
- [2] 傅德胜,王建荣.基于H.264的视频水印技术[J].计算机应用,2009,29(4):1174-1176.
- [3] 孙文静.基于能量差比率的DEW视频水印算法[J].计算机科学,2010,37(5):271-273.
- [4] 许拔,张仲明,何英亮,等.基于LDPC码的自适应视频水印算法研究[J].信号处理,2010,29(3):441-447.

(上接第1504页)

NPCR值基本稳定在0.99左右,UACI也在0.23附近波动。第一轮的NPCR和UACI值比理论值低的原因是改变的1位数据是在明文的最后,也即自适应结构的最后一次加密,所以只影响到IRB和ILB两个子块。

表3 明文改变1位后的NPCR和UACI

轮数	Lena		清明上河图	
	NPCR	UACI	NPCR	UACI
1	0.49780	0.16695	0.49564	0.16646
2	0.99610	0.33521	0.99589	0.33555
3	0.99625	0.33443	0.99626	0.33417
4	0.99594	0.33414	0.99603	0.33467

3.5 性能分析

在灰度扩散中,对每一个像素灰度值采用简单的加、模和异或运算,时间复杂度为 $O(n^2)$ 。另外,每一次子分块加密只需构造一个与前一子块大小相等的辅助矩阵A,而且只要两轮加密便可以达到所要求的性能。

4 结语

本文提出了一种新的自适应结构和灰度扩散机制。自适应结构使得对明文的微小改变能迅速地扩散到整个密文中。灰度扩散机制使得明文的统计信息被隐藏,能有效抵抗统计分析攻击。实验结果表明,该算法具有很强的鲁棒性和对密钥的敏感性,能够有效地抵抗统计分析、穷举攻击和差分攻击。

参考文献:

- [1] CHEN GUANRONG, MAO YAOBIN, CHUI C K. A symmetric im-

- [5] 楼偶俊,王相海.提升方案小波和HVS下的自适应视频水印算法研究[J].小型微型计算机系统,2008,29(4):734-740.
- [6] 郑振东,王沛,李莉.基于运动矢量域与DCT域的混合视频水印方案[J].中国图象图形学报,2009,14(12):2631-2634.
- [7] 杨高波,李俊杰,王小静,等.基于脆弱水印的H.264视频流完整性认证[J].湖南大学学报:自然科学版,2009,36(6):67-71.
- [8] 朱德庆,金光华.基于运动矢量的鲁棒视频水印算法[J].浙江大学学报:理学版,2010,37(3):286-290.
- [9] 张桂东,茅耀斌,王执铨.一种基于运动矢量的视频水印方案[J].中山大学学报,2004,43(2):117-119.
- [10] 王美华,裴庆祺,范科峰.基于脆弱水印的H.264视频完整性认证方案[J].西安电子科技大学学报,2007,34(5):823-826.
- [11] PROFROCK D, RICHTER H, SCHLAUWEG M. H.264/AVC video authentication using skipped macroblocks for an erasable watermark [C]// Proceedings of SPIE Visual Communications and Image Processing, 2009, 5960: 1480-1489.
- [12] DONOHO D. Compressed sensing [J]. IEEE Transactions on Information Theory, 2006, 52(4): 1289-1306.
- [13] VALENZISE G, TAGLIASACCHI M, TUBARO S. A compressive sensing based watermarking scheme for sparse image tampering identification [C]// Proceedings of the 16th IEEE International Conference on Image Processing, Washington, DC: IEEE, 2009: 1265-1268.
- [14] RICHARD B, MARK D, RONALD D. A simple proof of the restricted isometry property for random matrices [J]. Constructive Approximation, 2008, 28(3): 253-263.
- [15] GUAN ZHIHONG, HUANG FANGJUN, GUAN WENJIE. Chaos-based image encryption algorithm [J]. Physics Letters A, 2005, 346(1/2/3): 153-157.
- [16] ZHANG LINHUA, LIAO XIAOFENG, WANG XUEBING. An image encryption approach based on chaotic maps [J]. Chaos, Solitons & Fractals, 2005, 24(3): 759-765.
- [17] WONG K W, KWOK B S H, YUAN C H. An efficient diffusion approach for chaos-based image encryption [J]. Chaos, Solitons & Fractals, 2009, 41(5): 2652-2663.
- [18] HUANG C K, NIEN H H. Multi chaotic systems based pixel shuffle for image encryption [J]. Optics Communications, 2009, 282(11): 2123-2127.
- [19] 邓绍江,张岱固,濮忠良.一种基于混沌的图像置乱算法[J].计算机科学,2008,35(8):238-240.
- [20] 邓绍江,李艳涛,张岱固,等.一种基于混沌的JPEG2000图像加密算法.计算机科学,2009,36(5):273-275.
- [21] 廖晓峰,肖迪,陈勇,等.混沌密码学原理及其应用[M].北京:科学出版社,2009.
- [22] CHEN GANG, ZHAO XIAOYU, LI JUNLI. A self-adaptive algorithm on image encryption [J]. Journal of Software, 2005, 19(11): 1975-1974.
- [23] 周庆,胡月,廖晓峰.一种自适应的图像加密算法的分析及改进[J].电子学报,2009,37(12):2730-2734.
- [24] 赖师悦,廖晓峰,周庆.新的基于波传播的图像加密算法[J].计算机应用,2009,29(8):2210-2212.