

采用可逆水印的 HEVC 视频完整性认证方案

董晓慧, 林其伟, 许东旭

(华侨大学 信息科学与工程学院, 福建 厦门 361021)

摘要: 针对最新的视频编码标准 HEVC/H. 265, 提出一种基于可逆水印的视频完整性认证方案. 首先, 算法根据第一个 I 帧中相邻块的直流系数 (DC) 系数之间的大小关系提取特征码; 然后, 从第二个图像组 (GOP) 的 P 帧开始, 通过修改运动矢量某一分量的幅值嵌入水印, 并且把修改前幅值的最低有效位信息嵌入到该块最后一个离散余弦转换 (DCT) 系数上以实现视频还原. 实验结果表明: 算法简单有效, 具有较好的脆弱性, 同时能够对视频进行无失真还原.

关键词: 运动矢量; 离散余弦转换; HEVC/H. 265; 完整性认证; 可逆水印

中图分类号: TP 391

文献标志码: A

数字化和互联网技术正在以令人震惊的速度和规模发展, 使得数字多媒体产业的面貌发生翻天覆地的变化. 然而在享受它们带来的便利的同时, 也常常不得不接受盗版侵权和内容恶意篡改现象所带来的困扰. 因此, 数字多媒体产品的版权保护和内容认证成为急需解决的重要问题^[1], 而视频水印技术是一种非常有效的解决方案. 目前的视频正向着高清分辨率甚至超清分辨率发展, 而现有的视频编码技术已经远远不能满足消费者的需求^[2]. 完整性认证是一种发现信息篡改, 验证信息完整性、真实性的技术. 可实现完整性认证的技术有数字签名和数字水印技术. 用于认证的数字水印技术可分为脆弱水印和半脆弱水印两种^[3]. 国内外尚未见关于 HEVC 可逆视频水印方案, 文献^[4-6]也只涉及信息隐藏, 现有的可逆水印方案大多是基于 H. 264 的. 文献^[7-10]在一个宏块中嵌入多比特的其他宏块信息, 以在解码时对受损数据进行恢复或估计. Huo 等^[11]提出在 H. 264 中, 根据 4×4 块的预测模式分布, 采用“和不变”的方法嵌入可逆水印. Lin 等^[12]提出在 H. 264/AVC 基础上, 利用相邻宏块的残差量化后的 (discrete cosine transformation, DCT) 系数值预测当前块的值, 并利用预测差值的直方图平移嵌入水印. Liu 等^[13]在一个量化后的离散余弦转换 DCT 系数上嵌入水印, 使用耦合系数进行补偿, 从而消除误差漂移. 张维伟等^[14]将当前宏块 DCT 系数的哈希值作为水印嵌入到下一个相邻宏块中, 水印提取的同时对当前块进行数据还原. 本文结合 HEVC/H. 265 的新特点, 创新性地提出一种基于 HEVC/H. 265 的可逆视频水印方案.

1 HEVC/H. 265 变换、量化和帧间预测

1.1 HEVC/H. 265 中的变换和量化

HEVC/H. 265 和 H. 264 类似, 对预测残差也进行 DCT 整数变换. 不同的是 H. 264 只固定采用了 4×4 块 DCT 变换尺寸, 而 HEVC/H. 265 中则以变换单元 (TU) 进行变换和量化, DCT 变换的尺寸可以更加灵活地在 32×32 块到 4×4 块之间取值. 此外, HEVC/H. 265 还创新性采用 4×4 块离散正弦变换 (discrete sine transform, DST), 不过仅将它用于 4×4 块的帧内预测残差的编码. HEVC/H. 265 与 H. 264 的量化过程一样, 都是在整数 DCT 变换时一并完成的, 并且量化步长有 52 个等级 (0~51). 此外, HEVC/H. 265 也使用了率失真优化的量化 (rate distortion optimized quantization, RDOQ) 技术, 从

收稿日期: 2014-07-31

通信作者: 林其伟 (1959-), 男, 副教授, 博士, 主要从事视频编码与网络通信方式的研究. E-mail: qwlin@hqu.edu.cn.

基金项目: 福建省自然科学基金资助项目 (2012J01275)

而在给定码率的情况下选择最优的 Quantitative parameters(QP)使重建图像失真最小。

与 H. 264 不同的是, HEVC/H. 265 在 TU 中分别对亮度和色度分量进行量化操作. 在 TU 中, 所有变换系数都按照一个特定的 QP 统一进行量化和反量化. 这使得 HEVC/H. 265 的 RDOQ 比 H. 264 提高约 5% 的编码效率(亮度), 但会增加计算复杂度. 与 H. 264 采用的 Zig-Zag 扫描方法不同, HEVC/H. 265 将一个大的 TU 分成若干个 4×4 块系数组, 如果 TU 采用帧内预测模式, 则根据帧内预测方向自适应选择水平、垂直和对角 3 种方式中的一种, 如果 TU 采用的是帧间预测模式, 则只能使用对角扫描方式。

1.2 HEVC/H. 265 帧间预测

HEVC/H. 265 在 H. 264 基础上主要进行了以下 2 点改进。

1) 帧间预测时, 允许 CU 对称或非对称地划分为更小的 PU, PU 可以为方形, 也可以是矩形. 这使得 PU 在运动估计和运动补偿中更精确地符合图像中运动目标的形状, 而不需要进一步细分来解决。

2) HEVC/H. 265 对运动参数的编码有 Inter、改进的 Skip 和 Merge 3 种模式. 前两种与 H. 264 类似, Merge 模式是 HEVC/H. 265 新引入的一种运动合并技术, 对邻近的 PU 进行合并处理, 从而传输一次运动参数即可. 对 HEVC/H. 265 中的 Skip 模式, 编码器只需编码运动合并候选者的索引信息, 以保证解码时 Skip PU 可以拷贝中选者的运动参数作为自己的参数。

2 水印信息生成

对于生成水印信息的特征码, 要求其具有稳定性^[15], 特征码的生成和嵌入不应该选在同一帧. 这样能够避免因为选择区域相同, 给特征码生成及水印提取带来不稳定因素. 因此, 文中选择在第一个 I 帧提取特征码并且通过密钥加密, 进而生成水印信息, 因为 I 帧采用帧内编码, 是视频编码中最重要的一环, 比 P 帧更具有稳定性. 此外, 由于算法是在编码端嵌入水印的方案, 经过编码压缩形成码流, 在解码端通过解码器提取水印信息, 因而要求特征码对视频压缩具有鲁棒. 统计表明: 图像的直流系数 (dc coefficients, DC) 系数对于不同的压缩情况, 相邻两位仍然基本保持大小不变, 因此, 文中充分利用这一特点来构造特征码. 具体有如下 3 个生成过程。

1) 将第一个 I 帧的视频图像分一个个 DCT 变换块。

2) 找出每个块的 DC 系数, 比较相邻两个 DC 系数 DC_j 和 DC_{j+1} 的大小, 即

$$\left. \begin{aligned} DC_j \geq DC_{j+1}, & \quad M_j = 1, \\ DC_j < DC_{j+1}, & \quad M_j = 0. \end{aligned} \right\} \quad (1)$$

产生的特征码序列为 $M = \{M_1, M_2, \dots, M_{n-1}\}$.

3) 对特征码加密生成水印信息, 有

$$w_j = M_j \oplus p_j. \quad (2)$$

式(2)中: \oplus 为异或操作; p_j 是伪随机序列; 最终生成待嵌入水印序列为 $w = \{w_1, w_2, \dots, w_{n-1}\}$.

3 可逆水印的嵌入过程

3.1 水印嵌入位置选择

由于在 P 帧的运动矢量上嵌入水印有利于保证水印的脆弱性, 并且 P 帧的编码要参考 I 帧, 因此, 在 P 帧嵌入认证水印也能认证 I 帧的完整性. 文中选择从第二个图像组(GOP)的第一个 P 帧开始, 在它之后每个 P 帧都嵌入水印信息, 通过修改 P 帧运动矢量某一分量的幅值进行水印嵌入. 为了实现视频无失真还原, 将修改前分量幅值的最低有效位信息(LSB)嵌入到 DCT 量化后的最后一个系数(LN)上。

3.2 水印嵌入算法

具体嵌入步骤有如下 3 个步骤。

步骤 1 在 P 帧视频码流中, 对于运动参数编码方式为 Skip/Merge 的块进行跳过处理, 同时全零块也跳过, 不进行水印嵌入. 这是因为 Skip 编码的块没有运动矢量和残差信息, 而 Merge 编码的块不进行运动估计, 若修改会造成较大的率失真性能损失. 然后, 对剩下的每个非 Skip/Merge 编码的块嵌

入 1 bit 水印信息.

步骤 2 选择 P 帧运动矢量中 x 方向运动分量幅值 V_x , 修改该分量以实现水印嵌入的公式为

$$V'_x = V_x - \text{mod}(V_x, 2) + \omega. \quad (3)$$

式(3)中: V_x 和 V'_x 分别为修改前后 x 分量的幅值; ω 为水印信息.

步骤 3 将修改前分量幅值的最低有效位信息嵌入到该块量化后的最后一个 DCT 系数上, 即

$$\text{LN}' = 2 \times \text{LN} + \text{LSB}(V_x). \quad (4)$$

式(4)中: LN' 和 LN 分别为修改前后 DCT 变换块的最后一位系数; $\text{LSB}(V_x)$ 表示修改前运动矢量分量幅值的最低有效位信息.

4 水印的提取

水印提取即水印嵌入的逆过程为盲提取, 提取方法简单, 不需要原始视频. 算法水印的提取位置在解码端熵解码之后进行. 由系数值提取运动矢量分量幅值的最低有效位信息, 再根据提取到的 LSB 信息和运动矢量分量的幅值信息一起进一步提取出水印. 水印提取有如下 3 个规则.

1) 对 HEVC/H. 265 压缩码流进行解码, 得到每个 DCT 块反量化前的系数和运动矢量信息.

2) 由嵌入公式可知, V_x 的奇偶性和 LN' 是一致的, 因此, 提取出水印嵌入之前运动矢量分量幅值的最低有效位信息的公式为

$$\text{LSB}(V_x) = \text{mod}(\text{LN}', 2). \quad (8)$$

3) 同样地, 由于在水印嵌入时, 嵌入公式是将 V_x 的奇偶性改成与当前水印位一致, 因此, 提取水印信息的公式为

$$\omega = \text{mod}(V'_x, 2). \quad (9)$$

5 视频还原

视频还原可按照水印嵌入公式的逆变换进行. 具体有如下 2 个步骤.

步骤 1 根据解码端的 DCT 系数最后一位数值和提取出来的 V_x 最低有效位信息, 还原出原始的 DCT 最后一位系数值, 即

$$\text{LN} = \frac{\text{LN}' - \text{LSB}(V_x)}{2}. \quad (10)$$

步骤 2 无失真地恢复出原始的运动矢量的分量信息, 即

$$V_x = V'_x + \text{mod}(V_x, 2) - \omega. \quad (11)$$

6 实验结果与分析

为了验证算法的有效性和性能, 利用 HEVC/H. 265 测试平台 HM12.0 进行仿真实验. 实验中使用了 5 个不同的典型标准测试序列: PeopleOnStreet, Traffic, ParkScene, BQTerrace 和 Vidyo3. 参考软件配置参数如表 1 所示.

表 1 HM 的主要参数配置

Tab. 1 Configuration parameters of the HM

Parameters	Configuration	Parameters	Configuration
Profile	encoder_lowdelay_P_main	Intra period	4
Sequence type	"I PPP I ..."	QP	20
Frames to be encoded	40	FrameSkip	0
Frame rate/fps	30	RD optimization	1: on

6.1 水印嵌入的影响

3 个测试序列在嵌入水印和进行视频还原前后的视频图像, 如图 1 所示. 由图 1 可知: 在水印嵌入前后, 人眼几乎察觉不出视频质量的变化, 从主观上证明了算法满足水印的不可见性.



(a) ParkScene 原始视频图像



(b) BQTerrace 原始视频图像



(c) Vidyo3 原始视频图像



(d) ParkScene 含水印的视频图像



(e) BQTerrace 含水印的视频图像



(f) Vidyo3 含水印的视频图像



(g) ParkScene 还原后视频图像



(h) BQTerrace 还原后视频图像



(i) Vidyo3 还原后视频图像

图 1 水印嵌入前后和视频还原前后视频图像质量对比

Fig. 1 Comparison of the visual quality between the original and the marked frames

5 个不同的测试序列在水印嵌入前后(未经过还原模块)的 $R_{SN,2}$ 、经过还原模块的 $R_{SN,2}$ 、比特率(η)、水印容量(C)以及编码时间(t)的对比情况,如表 2 所示.表 2 中:符号“+”表示嵌入水印之后相对于原始是增加的;符号“-”表示嵌入水印之后相对于原始是降低的.

表 2 对测试序列的实验结果

Tab. 2 Experimental result for test sequence

测试序列	$R_{SN,1}/dB$	$R_{SN,2}/dB$	$\eta/\%$	$t/\%$	C/bit
PeopleOnStreet	-0.32	0	+0.006	+0.97	2 425
Traffic	-0.22	0	+0.009	+0.34	1 495
ParkScene	-0.28	0	+0.008	+0.07	750
Vidyo3	-0.18	0	+0.003	+0.25	280
BQTerrace	-0.17	0	+0.001	+0.87	1 100

由表 2 可知:编码时间的增加量都在 1%以内,说明水印的嵌入对编码时间影响很小;而 R_{SN} 和码率也仅有微小的变化,从客观上证明了算法水印嵌入对视频质量影响很小.这是因为 HEVC/H. 265 含有很多 Skip/Merge 编码的块,越是运动平缓的视频,其中含有的 Skip/Merge 编码的块越多.

统计数据如表 3 所示.而算法对这类块没有作任何修改,即使在修改的块中,对运动矢量分量的幅值修改量也不会超过 1.因此,对视频本身的影响也较小,这也正是在运动剧烈且分辨率较高的视频序列中水印嵌入容量较大,而在运动平缓和分辨率较低的的视频中容量较小的原因.经过还原的视频 R_{SN} 和原始完全一样,证明了算法的可逆性.

表3 Skip和Merge编码块所占比重
Tab.3 Proportion of code blocks using Skip/Merge mode

Sequences	QP=20		Sequences	QP=20	
	Depth	$\eta/\%$		Depth	$\eta/\%$
PeopleOnStreet 2 560×1 600	0	42.8	Vidyo3 1 280×720	0	81.9
	1	43.0		1	86.8
	2	55.6		2	91.3
	3	67.0		3	94.2
Traffic 2 650×1 600	0	72.2	BQTerrace 1 920×1 080	0	65.8
	1	76.0		1	69.7
	2	84.8		2	74.2
	3	91.1		3	77.2
ParkScene 1 920×1 080	0	63.9			
	1	71.6			
	2	81.1			
	3	88.2			

6.2 完整性认证

当正确提取率(δ)小于某个阈值时,可认为完整性认证结果为“不完整”.实验中阈值设为0.999,分别使用了运动剧烈序列 PeopleOnStreet、运动平缓序列 Vidyo3 和中等剧烈视频 ParkScene 3个典型测试序列.在不同QP下含水印视频遭受攻击后的完整性认证情况,如表4所示.表4中:“True”表示认证结果为“完整”;“False”表示认证结果为“不完整”.实验验证了第2个GOP的完整性.

表4 完整性认证实验结果

Tab.4 Experimental results of integrity authentication

攻击类型	PeopleOnStreet		Vidyo3		ParkScene		
	QP=20	$\delta/\%$	认证结果	$\delta/\%$	认证结果	$\delta/\%$	认证结果
无攻击	100	100	True	100	True	100	True
重编码	3	3	False	3	False	3	False
高斯噪声(0,0.01)	7	7	False	7	False	6	False
椒盐噪声(0.005)	6	6	False	6	False	6	False
帧剪切	3	3	False	3	False	3	False

由表4可知:在未遭到攻击时,算法能正确提取出水印,在遭受攻击时,水印不能被正确提取,而且正确提取率较低说明了算法在认证视频完整性方面灵敏有效.

7 结论

提出了一种基于 HEVC/H.265 的视频可逆脆弱水印算法,算法通过从 I 帧提取特征码作为水印嵌入到 P 帧运动矢量的某个分量当中,对该分量的修改量很小,保证了视频即使通过普通解码器解码,人眼也很难察觉水印嵌入前后视频图像的差异.

利用高频 DCT 系数来记录修改前的信息以实现视频无失真还原.因此,通过含有还原模块的解码器,可以做到对视频质量完全无影响,在一些特定场合依然不影响视频使用.算法在 R_{SN} 、比特率、编码时间及水印嵌入容量上能取得较好的折中,并且水印的脆弱性是由 P 帧运动矢量的脆弱性保证的,具有较高的敏感度.

参考文献:

- [1] 孙圣和,陆哲明.数字水印处理技术[J].电子学报,2000,8(8):85-90.
- [2] 李恒忠,崔建明,郭勇,等.基于 HEVC/H.265 视频标准的熵编码过程[J].电脑知识与技术,2013,9(14):3356-3359.
- [3] COX I J, MILLER M L. The first 50 years of electronic watermarking[J]. EURASIP Journal on Applied Signal Pro-

- cessing, 2002, 2002(1):126-132.
- [4] CHANG P C, CHUNG K L, CHEN J J, et al. A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames[J]. *Journal of Visual Communication and Image Representation*, 2014, 25(2):239-253.
- [5] WANG Jiaji, WANG Rangding, LI Wei. A Large-capacity information hiding method for HEVC video[C]//3rd International Conference on Computer Science and Service System. Atlantis; Bangkok Press, 2014:934-937.
- [6] WANG Jing, YU Xiang, DAKE H E D, et al. Multiple sign bits hiding for high efficiency video coding[C]//Visual Communications and Image Processing[C]//San Diego; IEEE Press, 2012:1-6.
- [7] PROFROCK D, RICHTER H, SCHLAUWEG M, et al. H. 264/AVC video authentication using skipped macroblocks for an erasable watermark[J]. *Proceeding of SPIE Visual Communications and Image Processing*. Beijing: IEEE Press, 2005:1480-1489.
- [8] CHUNG Kuoliang, HUANG Yonghuai, CHANG Pochun, et al. Reversible data hiding-based approach for intra-frame error concealment in H. 264/AVC[J]. *IEEE Transactions on Circuits and System for Video Technology*, 2010, 20(11):1643-1647.
- [9] LIE W N, LIN T C, TSAI D C, et al. Error resilient coding based on reversible data embedding technique for H. 264/AVC video[C]//Proceedings of IEEE International Conference on Multimedia and Expo. Amsterdam; IEEE Press, 2005:1174-1177.
- [10] LIN S D, MENG H C, SU Y L. A novel error resilience using reversible data embedding in H. 264/AVC[C]//International Conference on Information, Communications and Signal Processing. Singapore; IEEE Press, 2007:1-5.
- [11] HUO Weijing, ZHU Yuesheng. A reversible watermarking algorithm with error-drift elimination in H. 264/AVC stream[C]//Proceedings of International Conference on Consumer Electronics, Communications and Networks. Xianning; IEEE Press, 2011:2893-2896.
- [12] LIN Y C, LI J H. Reversible watermarking for H. 264/AVC videos[J]. *World Academic of Science, Engineering and Technology*, 2011, 78:828-831.
- [13] LIU Yunxia, LI Zhitang, MA Xiaojing. Reversible data hiding scheme based on H. 264/AVC without distortion drift[J]. *Journal of Software*, 2012, 7(5):1059-1065.
- [14] ZHANG Weiwei, ZHANG Ru, LIU Jianyi, et al. A reversible fragile video watermarking for H. 264/AVC[J]. *Journal of Electronics and Information Technology*, 2013, 35(1):106-112.
- [15] 吴国楨, 冯桂. 一种基于 H. 264 半脆弱视频水印方案[J]. *通信技术*, 2012, 1(45):112-118.

Scheme of Video Integrity Authentication Based on Reversible Watermarking for HEVC

DONG Xiaohui, LIN Qiwei, XU Dongxu

(College of Information Science and Engineering, Huaqiao University, Xiamen 361021, China)

Abstract: An algorithm of reversible watermarking based on new video coding standard HEVC/H. 265 is proposed in this paper. The proposed algorithm firstly compares the DC coefficients coefficient of contiguous two blocks in the first I frame to create an authentication code. Secondly, embed the code as watermark into P frames from the second group of pictures by modifying one motion vector component amplitude, then embed the least significant bit of the original MV amplitude into the last coefficient of the discrete cosine transformation block to restore original video. Experimental results show that the proposed algorithm has good fragility and is easily to be extracted from the video, what's more, it can restore the video exactly.

Keywords: motion vector; discrete cosine transformation; HEVC/H. 265; integrity authentication; reversible watermarking