Watermarking in H.264/AVC Compressed Domain Using CAVLC

Qian Li
College of Information Science and Engineering,Ningbo University,Ningbo 315211,China
Email: liqian_mine@126.com

Rangding Wang
College of Information Science and Engineering,Ningbo University,Ningbo 315211,China
Email: wangrangding@nbu.edu.cn

***Abstract*—A new real-time watermarking technique based on H.264/AVC video standard is proposed. The algorithm works in the compressed domain by embedding watermark bits into quantized DCT coefficients of 4×4 blocks of the I-frame during the Context-based Adaptive Variable Length Coding (CAVLC) process. CAVLC offers a lower computational complexity which is efficient to the algorithm. During watermark extraction, the entire video do not need to be decoded,which meets the requirement of the real-time processing.The scheme yields tiny bit-rate change after watermarking and the degradation of video quality is negligible. The simulation results show that watermark embedded is fragile and is easily distorted under attacks, which can be used for the video authentication or covert communication applications.**

***Index Terms*—H.264/AVC, CAVLC, Watermarking, Video authentication**

I. INTRODUCTION

With the fast developing of multimedia network technology, the digital media reached an unprecedented level. However, the video information is vulnerable to tampering attacks during transmission.The case of illegally tampering of digital video are becoming an increasingly serious problem. Therefore, in recent years, how to implement effective protection of the authenticity and integrity of the video content in a network environment has become the hot spot research in the field of multimedia information security [1], and promoted the rapid development of digital watermarking technology. The watermark information, such as data and images, embedded into the multimedia cover utilize the HVS (human visual system) and the redundancy of digital content, does not change the external characteristics and practical value of the carrier.And it should make sure that human sense organs cannot feel the change of the carrier. By extracting the watermark information, we can verify the integrity of the video content. Fig. 1 shows the basic procedure of watermark embedding.

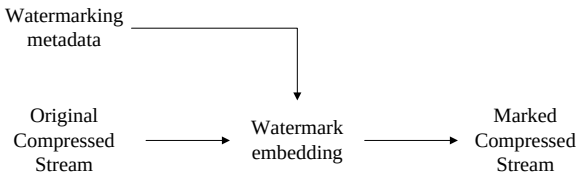

Figure 1. Watermark embedding procedure

In the figure, the embed procedure has two inputs, the H.264/AVC video stream and some watermarking metadata, and then form the marked compressed stream. In the whole process, the imperceptibility of the video should be kept. According to the function, the purpose of the watermark can be divided into two kinds as follows.

1. Robustness: Generally, robust watermarking can resist to such as compression, geometric transformation, collusion attacks or other malicious attack, which is used for copyright protection, copy control and so on.

2. Fragile: Fragile watermark is one class of authentication watermarks, usually get distorted, altered and even completely destroyed in the presence of attacks, which can detect small changes of the multimedia data, and then indication video content has been changed or damaged.

H.264/AVC is a new video coding standard jointly developed by the ITU-T Video Coding Experts Group (VCEG) and the ISO/IEC Moving Picture Experts Group (MPEG) standards committees. The main goals of the standardization effort have been enhanced the compression performance and "network-friendly" [2]. H.264/AVC achieves a higher coding performance than the previous video coding standards, such as MPEG-2 and MPEG-4. In order to achieve this performance, H.264/AVC adopts various advanced techniques, such as variable block-size motion estimation, multiple reference frame motion estimation, spatial intra-prediction, and novel entropy coding. Fig. 2 and Fig. 3 show the encoder and decoder of the H.264/AVC respectively.

Manuscript received March 27, 2013; revised April 9, 2013; accepted April 25, 2013.

Corresponding author：Rangding Wang.
Email：wangrangding@nbu.edu.cn

doi:10.4304/jcp.8.12.3126-3133

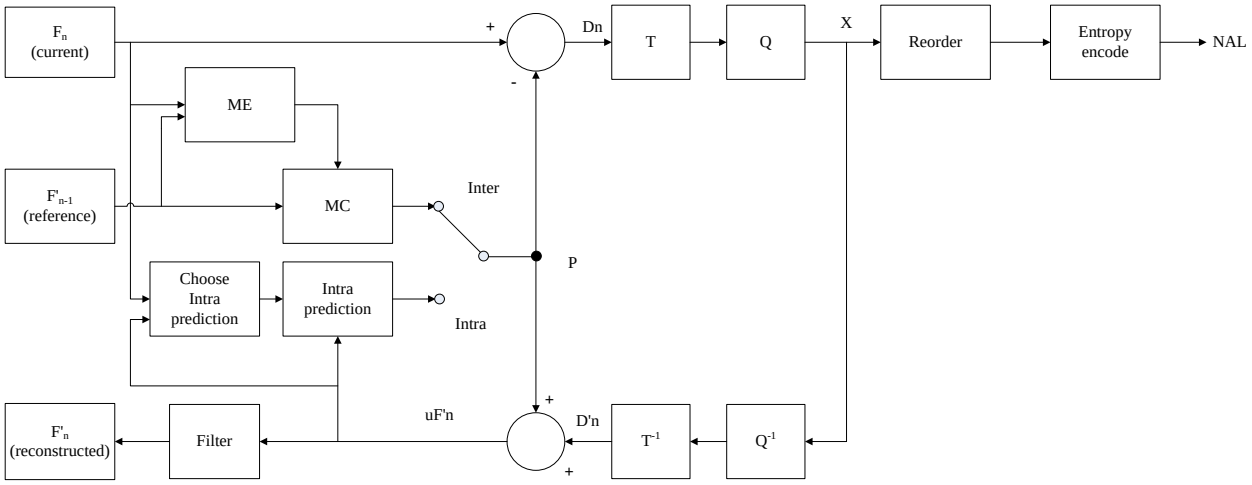

Figure 2. The H.264/AVC encoder

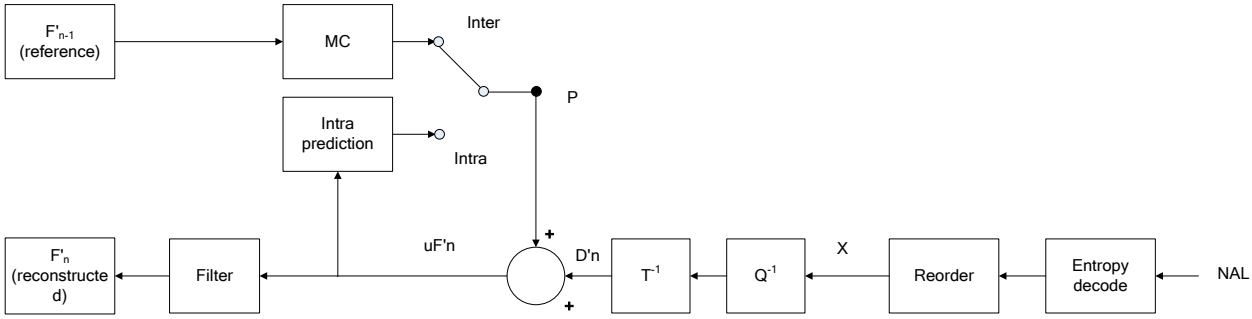

Figure 3. The H.264/AVC decoder

The encoder includes two dataflow paths, a "forward" path (left to right) and a "reconstruction" path (right to left). In forward path, an input frame F_n is presented for encoding, the frame is processed in units of a macroblock (corresponding to 16×16 pixels in the original image), each macroblock is encoded in intra or inter mode. In either case, a prediction macroblock P is formed based on a reconstructed frame [3]. The residual macroblock D_n is subtracted from the prediction P and the current macroblock. And then the D_n will be transformed and quantized to give a set of quantized transform coefficients X. These coefficients are re-ordered and entropy encoded.

The encoder has the following several major components. And we will introduce several digital video watermarking schemes suitable for the H.264/AVC video compression standard.

1. Intra prediction. Intra prediction is a unique technology in H.264/AVC, which can reduce the spatial redundancy effectively and achieve a higher compression rate. It can be divided into intra_4×4 prediction and intra_16×16 prediction according to the size of predicting block. There are nine kinds of prediction modes for intra_4×4 and four kinds of prediction modes of intra_16×16, so some researchers proposed to embed the watermark information by modulating the coding mode [4-7]. These schemes usually are used for the large capacity steganography.

Zhu [5] proposed an information hiding method based on predicting difference by analyzing the intra_4×4 prediction modes (I4-modes). The algorithm first divided the I4-modes into two groups to form the rule of mapping between these modes and the bits to be embedded, and then modulated the I4-modes by the rule of mapping to implement the hiding of information. The hiding algorithm in [6] is the improvement of [5], in addition to the I4-modes, also modified the intra_16×16 prediction modes (I16-modes) to hiding information. In Ref. [7], the secret information is embedded by modifying the prediction modes of 4×4 luminance blocks. If the best mode does not match the information bit, the prediction mode should be modified by replacing the best mode with the substitute mode.

2. Inter prediction. Inter prediction creates a prediction model from one or more previously encoded video frames.

Each partition in an inter-coded macroblock is predicted from an area of the same size in a reference picture. For each part of the frame, encoder chooses the best partition size, and for each partition performs motion estimation and motion compensation[8]. There are some watermarking algorithms based on motion vectors (MV) [9-13]. Due to the motion vectors are very sensitive to signal processing attacks, these methods are generally fragile.

Kuo et al [12] took advantage of the parity of 1/4 pixel motion vector horizontal and vertical coordinate values embedding watermark information. Through statistical analysis of the different amplitude of the MV, the smaller motion vectors are chosen to embedded watermark by modulating the 1/4 pixel search points. In Ref. [13], the algorithm first generated authentication code according to the encoding mode of macroblock, and then embedded them into video frame by the modulation of the MV. During the process of modulating introduce the rate distortion cost to achieve a better balance of rate-distortion.

3. Discrete Cosine Transform (DCT). Each residual macroblock is transformed, quantized and coded. Different from the previous standards such as MPEG-1, MPEG-2, MPEG-4 and H.263 use 8×8 transform, the H.264 made use of the 4×4 blocks transform instead. Some researchers embedded the robust watermark information into the quantized DCT coefficients, which can be used for copyright protection [14-17].

In Ref. [15], the author points out that in a compressed video, the P-frames were highly compressed by motion compensation, and the P-frames appear more frequently in the compressed video and their watermarking capacity should be exploited. So they embed the watermark to nonzero-quantized ac residuals in P-frames. The experimental results show that the video watermark detection algorithm has controllable performance, and high robustness to several different attacks. Noorkami [16] proposed a robust watermarking algorithm for H.264. The watermark information was embedded in a selected subset of the quantized DCT coefficients. The author used a key-dependent algorithm to select a subset of the coefficients with visual watermarking capacity for watermark embedding to obtain robustness to malicious attacks.

4. Entropy coding. In H.264/AVC main profile, there are two kinds of entropy coding. One is CAVLC (Context-based Adaptive Variable Length Coding), and the other is CABAC (Context-Based Adaptive Binary Arithmetic Coding). CAVLC has lower compression efficiency than CABAC but also has a lower computational overhead. Ref. [18-24] take use of the process of entropy coding to achieve information hiding.

Ref. [18] proposed a digital watermarking to protect the ownership of a video content which is compressed by H.264/AVC main profile. It uses the contexts extracted during the context modeling process of CABAC to position the watermark bits by simply checking the context values and determining the coefficients. The algorithm has very high imperceptibility and robustness to the attacks. CAVLC is a new feature in H.264. At present, the CAVLC-based video watermarking mainly modify the number of Trailing Ones [21-22], or the sign bit of the Trailing Ones [23], or the parity of the last one non-zero coefficient [24]. In [24], the watermark bits embedded into quantized luminance 4×4 DCT blocks of I frames. Based on the CAVLC entropy coding technique, the algorithm only modifying the last non-zero coefficient in zig-zag order, has good transparency.

In this paper, a watermarking scheme during the CAVLC process was proposed. In our method, watermark information is embedded by replacing nonzero coefficients *level_prefix* sequence during CAVLC coding. One bit watermark is embedded in each satisfy the embedding condition of luma intra 4×4 blocks. The scheme can combines the H.264 standard closely and get the low computational complexity, meets the requirement of real-time processing perfectly. And achieve micro visual distortion for the reasons of the low differences between the replacement code and the original. Furthermore, the CAVLC high coding performance ensures the efficiency of the implementation of the watermarking algorithm.

The outline of the paper is as follows. In Section II, we indicate the location of the watermark embedding based on the CAVLC. Section III describes the specific watermarking method about how to embed and extract watermark bits. Section IV provides experimental results and analysis, aiming at demonstrating the validity of the proposed scheme. Finally, conclusions are drawn in Section V.

II. The Location of the Watermark Embedding Based on the CAVLC

In H.264/AVC coding process, the result from all the computations based on the 4×4 blocks is scanned in a zig-zag way to arrange the DCT coefficients in order. Then, the scanned result is encoded by entropy coding to reduce the statistical redundancy.

CAVLC is used to encode residual, zig-zag ordered 4×4 (and 2×2) blocks of transform coefficients. This method is designed to take advantage of several characteristics of quantized 4×4 blocks [3]. Firstly, after prediction, transform and quantization, blocks typically contain mostly zeros. CAVLC uses run-level coding to compactly represent strings of zeros. Secondly, the highest non-zero coefficients after the zig-zag scan are often sequences of +/-1. Thirdly, the number of non-zero coefficients in neighboring blocks is correlated. The number of coefficients is encoded using a look-up table.The choice of look-up table depends on the number of non-zero coefficients in neighboring blocks. Finally, the magnitude of non-zero coefficients tends to be larger toward the low frequency regions. CAVLC takes advantage of this by adapting the choice of VLC look-up table for the "level" parameter depending on recently-coded level magnitudes. Therefore, taking into consideration the above characteristics, CAVLC employs five syntax elements shown in Table I.

TABLE I

CAVLC SYNTAX ELEMENTS

Syntax Elements	Description
Coeff_token	Both the total number of non-zero coefficients (TotalCoeffs) and the number of trailing +/- 1 values (TrailingOnes)
Sign_of_TrailingOnes	A sign bit for each TrailingOnes in reverse zig-zag order
Level	The values of non-zero coefficients except for TrailingOnes
Total_zeros	The total number of zeros before the last coefficient
Run_before	The number of zeros proceeding each non-zero coefficient in reverse order

CAVLC code word can be expressed as the following format:

{Coeff_token, Sign_of_TrailingOnes, Level, Total_ zeros, Run_before}

Our scheme is proposed to embed the watermark information by modulating CAVLC code words. During the CAVLC modulation, not all syntax elements can be modified. For example, *Coeff_token* is one of them. There are four look-up tables used to encode *Coeff_token*, the choice of the table depends on the number of non-zero coefficients in the previously coded above and left blocks. If *Coeff_token* has been changed in one block, the damage caused by error propagation may be tremendous, and affects coding of neighboring blocks. Furthermore, altering *Total_zeros* and *Run_before* also has a similar problem. To maintain transparency and fidelity, all watermarking will take place in the combination of *{TrailingOnes, Sign_of_TrailingOnes, Level}*. In this work, we choose *Level* to embed the watermark information.

III. PROPOSED WATERMARKING ALGORITHM

In the process of CAVLC entropy coding, *Level* is encoded in the order from high to low frequency, each code word contains a *level_prefix* and a *level_suffix*, encoding process in Eq. (1)-(3).

$$\begin{cases} levelCode = (Level \ll 1) - 2 & if \quad Level > 0 \\ levelCode = -(Level \ll 1) - 1 & if \quad Level < 0 \end{cases} \quad (1)$$

$$level\_prefix = levelCode \,/(1 \ll suffixLength) \quad (2)$$

$$level\_suffix = levelCode\%(1 \ll suffixLength) \quad (3)$$

There is a codebook to encode *level_prefix*, show in Table II.

TABLE II

LEVEL_PREFIX CODEBOOK

level_prefix	bit string
0	1
1	01
2	001
3	0001
4	0000 1
…	……
12	0000 0000 0000 1
13	0000 0000 0000 01
14	0000 0000 0000 001

From Table II we know that the number of zero in *bit string* is the value of *level_prefix*, so we can replace the *bit string* sequences in some rules. In addition, we only choose *level_prefix* value between 0 and 14, and the replacement occurred in two adjacent sequences, the differences between the replacement code and the original is little, guarantee the quality of the video.

Replacement rule is according to Fig. 4, if the watermark bit is '0', modify the number of zero in *bit string (Numzero_prefix)* is even, otherwise, if the watermark bit is '1', then modify the number of zero is odd.

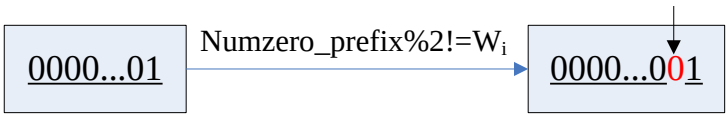

Figure 4. The Rule of the Code Replacement

A. Watermark Embedding

The watermark embedding is performed during the CAVLC entropy coding process, include several steps.

STEP1. Positioning the codeword of the non-zero coefficient in 4×4 residual luma block in the H.264 stream;

STEP2. If the data block has Trailing Ones, go to STEP3. If not, the last non-zero coefficient is Level, then replace the level_prefix sequence according to the above replacement rule;

STEP3. Repeat STEP1- STEP2 until the end of the video stream.

B. Watermark Extraction and Authentication

This scheme could extract the watermark quickly and simply, and do not need the original video stream for reference, the detail is described as follow.

STEP1. Positioning the watermarked block, detect one-bit-watermark from it by Eq. (4);

$$W_i' = \begin{cases} 1 & Numzero\_prefix \,\%\, 2 == 1 \\ 0 & Numzero\_prefix \,\%\, 2 == 0 \end{cases} \quad (4)$$

STEP2. Repeat STEP1 until watermarks are all extracted.

STEP3. Compare watermark W' to original W, if no bit has been changed we declared that the video is complete, otherwise the video has been tampered.

IV. Simulation Results and Analysis

The proposed watermark embedding scheme has been implemented in the H.264/AVC reference software version JM-8.6[25]. Four standard video sequences (Bus, Akiyo, Harbour and Highway) in QCIF format (176×144) are encoded and tested under various quantization parameters QP=[26,28,30]. Some important configuration parameters of the reference software are given in Table III. One binary image (42×39) is used as the digital watermark (shown in Fig. 5).

Figure 5. Watermarking Image

A. Effect on the Quality and Bit-rate of the Video

To evaluate the imperceptibility of the proposed scheme, as Fig. 6 and Fig. 7 illustrated, we compare the watermarked video with the original. There are little difference between the watermarked and the original image, so the algorithm meets the human perceptual requirement. Besides subjective observation, PSNR (Peak Signal to Noise Ratio) is usually taken to evaluate the perceptual quality. Fig. 8 illustrates the *Y*-PSNR (luma PSNR) comparison between the original and the watermarked video Bus, Akiyo, Harbour and Highway. The curves show that the PSNR of the embedded frames are slightly different from the original frames, demonstrate the watermark introduces little influence to the video.

TABLE III

THE MAIN CONFIGURE PARAMETERS FOR THE ENCODER

parameter	value
Profile	Main profile
Frames to be encoded	50
GOP	"IBPBPIBP…"
Intra-period	5
Entropy coding	CAVLC
RD optimization	use
Number Reference Frames	5
Frame rate	30fps

Figure 6. Original frames(sixth I-frame)

Figure 7. Watermarked frames(sixth I-frame)

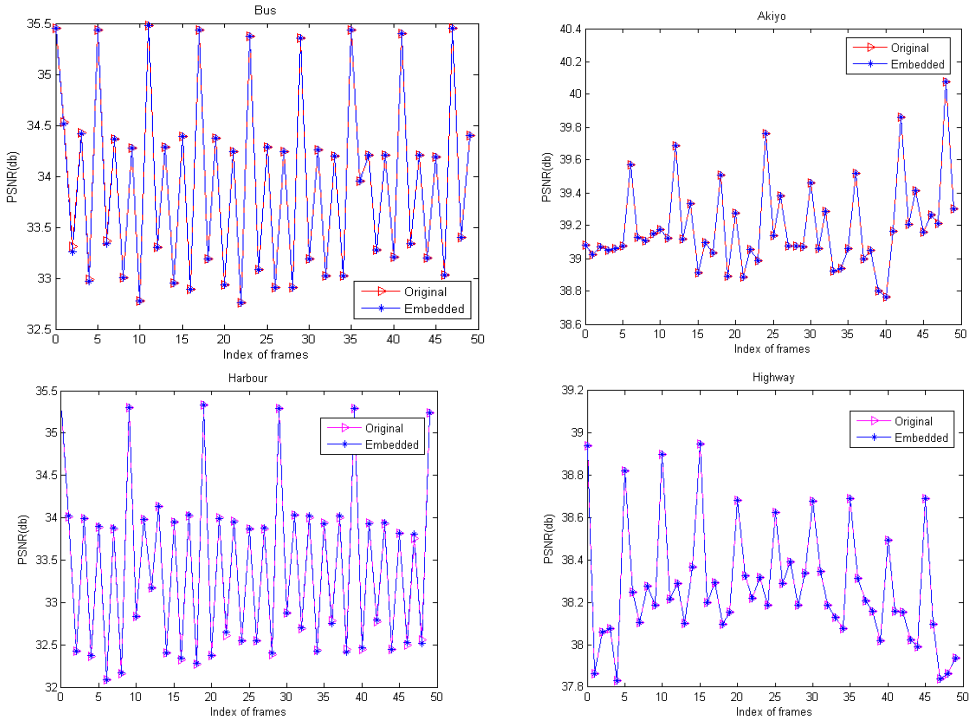

Figure 8. PSNR Comparison for QP=28

However, for different video contents, the PSNR cannot be a reliable method to evaluate the video quality. Taking into account the HVS characteristics, the paper also proposed to use another objective metric SSIM. SSIM represents the similarity of the video stream, in the range between 0 and 1, where 1 indicates the reference image and the target are identical. The value of SSIM and the bit rate R_{var} for the test sequences are shown in Table IV, where the R_{var} indicates the bit rate increasing percentage in video.

$$R_{\text{var}} = \frac{R' - R}{R} \times 100\% \quad (5)$$

Where R' and R denotes the bit-rate of the marked and the original video respectively.

TABLE IV

SSIM AND BIT-RATE FOR QP=26,28 AND 30

Sequence	Bus			Akiyo			Harbour			Highway		
QP	26	28	30	26	28	30	26	28	30	26	28	30
SSIM	0.9716	0.9742	0.9802	0.9821	0.9816	0.9832	0.9836	0.9769	0.9778	0.9801	0.9854	0.9834
R_{var}(%)	+0.04	+0.01	+0.05	+0.05	+0.02	+0.33	+0.03	+0.02	+0.12	+0.15	+0.22	+0.07

It can be seen from Table IV that the SSIM values are all above 0.97, which demonstrate that watermark embedding is almost no impact on video quality. There is little bit-rate increase, for the reasons of the little differences between the replacement and the original code.

B. Video Authentication

In order to test whether our method can verify the integrity of video content or not, we test the vulnerability of the proposed method. If the watermark information can be extracted correctly, denote the video is integrity; otherwise, if the watermark is destroyed, we belive that the video is under tampered. During analysis the vulnerability, it's more tend to estimate the sensitivity of the watermarked video towards varieties of minor attacks. In this paper, we attack our video under re-encoding, because if the watermark can not resist the attack of re-encoding, let alone other attacks. Table V illustrates the vulnerability results of the watermark, we find that the watermarks can be extracted completely with no attack to the video, and distorted while the video suffered any attacks, indicate the algorithm has a good vulnerability.

TABLE V

FRANGIBILITY RESULTS

Sequence	Original watermark	Without attack	Re-encoding
Bus			
Akiyo			
Harbour			
Highway			

V. CONCLUSION

In this paper, a watermarking algorithm for video integrity certification based on H.264/AVC is proposed. The algorithm uses the special coding process of the non-zero coefficient amplitude *level* during CAVLC, embedding watermarks by displacing the *level-prefix* sequence of the selected *Level*. Embedded information can be extracted blindly without need the original video sequence. Simulation results demonstrate that the algorithm can achieve a great imperceptibility as well as the slight bit-rate increase. The scheme is fragile, the watermark information will be lost if the watermarked video stream is decoded and re-encoded. It could be used for video authentication or covert communication.

ACKNOWLEDGEMENT

This work is supported by the National Natural Science Foundation of China (61170137), Doctoral Fund of Ministry of Education of China (20103305110002), Scientific Research Fund of Zhejiang Provincial Education Department (Y201119434), Zhejiang Provincial Natural Science Foundation of China (Y13F020071)，Key Innovation Team of Zhejiang Province (C01416124200), The Outstanding (Postgraduate) Dissertation Growth Foundation of Ningbo University (10Y20100002).

REFERENCES

[1] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk. Advances in digital video content protection. Proceedings of the IEEE,2005,93(l):171-183.

[2] T. Wiegand, G. J. Sullivan, G. Bjntegaard: ‘Overview of the H.264/AVC video coding standard’, IEEE Transactions on Circuits and Systems for Video Technology,2003,13,(7),560–576.

[3] H.264/MPEG-4 Part 10 White Paper. http://ftp3.itu.ch/av-arch/jvt-site/.

[4] C. H. Liu, O T. C. Chen. Data hiding in inter and intra prediction modes of H.264/AVC. IEEE International Symposium on Circuits and Systems (ISCAS 2008), 2008,pp. 3025–3028.

[5] H. L. Zhu, R. D. Wang, D. W. Xu, X. X. Zhou. Information Hiding Algorithm for H.264 Based on the predition difference of Intra_4×4. 2010 3rd International Congress on Image and Signal Processing (CISP2010),2010,pp.487-490.

[6] R. D. Wang, H. L. Zhu, D. W. Xu. Information Hiding Algorithm for H.264 Based on the Intra prediction difference. Journal of Information & Computational Science,2010,7(1):1-6.

[7] D.W. Xu, R. D. Wang, J. C. Wang. Prediction mode modulated data-hiding algorithm for H.264/AVC. Journal of Real-Time Image Processing, 2012,7(4):205-214.

[8] K. H. Nguyen, P. Cao, X. X. Wang. An Efficient Implementation of H.264/AVC Integer Motion Estimation Algorithm on Coarsegrained Reconfigurable Computing System. Journal Of Computers.2013,8(3):594-604.

[9] P. Wang, Z. D. Zheng and J Ying. A Novel Video Watermark Technique in Motion Vectors. 2008 International Conference on Audio, Language and Image Processing (ICALIP),2008,pp.1555-1559.

[10] H. A. Aly. Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error. IEEE Transactions on Information Forensics and Security, 2011, 6(1):14-18.

[11] G. Feng, G. Z. Wu. Motion Vector and Mode Selection Based Fragile Video Watermarking Algorithm. 2011 IEEE International Conference on Anti-Counterfeiting, Security and Identification (ASID),2011,pp.73-76.

[12] T. Y. Kuo, Y. C. Lo. Fragile video watermarking technique by motion field embedding with rate-distortion minimization. Journal of Communication and Computer,2009,6(1):16-22.

[13] R. D. Wang, Q. Li, H. L. Zhu, D. W. Xu. Fragile Watermarking Scheme Suitable for the Authentication of H.264/AVC Video Content. Journal of Information & Computational Science 2012,9(13):3693–3706.

[14] W. M. Chen，C. J. Lai，H. C. Wang, H. C. Chao, C. H. Lo. H.264 video watermarking with secret image sharing.IEEE International Symposium on Broadband Mu ltimedia Systems and Broadcasting, 2009:1-7.

[15] M. Noorkami, R. M. Mersereau. Digital video watermarking in P_frames with controlled video bit_rate increase. IEEE transactions on information forensics and security, 2008,3(3):441-455.

[16] M. Noorkami. A Framework for Robust Watermarking of H.264-Encoded Video with Controllable Detection Performance. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2007, 2(1):14-23.

[17] Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad. Video Watermarking Techniques for Copyright protection and Content Authentication. International Journal of Computer Information Systems and Industrial Management Applications. 2013, 5:652–660.

[18] D. K. Zou, J. A. Bloom. H.264/AVC Substitution Watermarking: A CAVLC Example. Media Forensics and Security,2009,72540Z:1-12.

[19] R. D. WANG ,L. J. HU, D. W. XU. A Watermarking Algorithm Based on the CABAC Entropy Coding for Journal of Computational Information Systems， 2011， 7：2132-2141.

[20] D. K. Zou, J. A. Bloom. H.264 Stream Replacement Watermarking With CABAC Encoding. IEEE International Conference on Multimedia and Expo (ICME), 2010,pp.117-121.

[21] K. Liao, S. G. Lian, Z. C. Guo. Efficient information hiding in H.264/AVC video coding. Telecommunication System,2012,49(2):261-269.
[22] D. W. Xu, R. D. Wang, J. C. Wang. Low Complexity Video Watermarking Algorithm by Exploiting CAVLC in H.264/AVC. 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS). 2010, pp.411-415.
[23] M. K. Sung, B. K. Sang, Y. Hong. Image Analysis and Recognition Lecture Notes in Computer Science, 2007, 4633: 698-707.
[24] A. A. Mohammad, A. E. Eran. A Semi-Fragile Watermarking Technique for H.264/AVC Using CAVLC. International Journal of Signal and Image Processing, 2010, Vol.1, pp.151-159.
[25] K. Suhring. H.264/AVC Joint Model 8.6 (JM-8.6) Reference Software [Online]. http://iphome.hhi.de/suehring/tml/.

Qian Li is born in 1986. She is currently the PhD student in College of Information Science and Engineering, Ningbo University, China. Her research interests mainly include network and information security, digital watermarking, information hiding, and video signal processing.

Rangding Wang is born in 1962. Received his M.S. degree in the Department of Computer Science and Engineering from the Northwest Polytechnic University, Xian in 1987, and received his Ph.D. degree in the School of Electronic and Information Engineering from Tongji University, Shanghai, China, in 2004. He is now a professor at Faculty of Information Science and Engineering, Ningbo University, China. His research interests mainly include multimedia security, digital watermarking for digital rights management, data hiding, and steganography for computer forensics.