http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (6): 1116-1124, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.1116.1124

Large Capacity Data Hiding Combined with Secure-intra-watermarking Based on H.264/AVC

Lujian Hu, Rangding Wang and Dawen Xu
CKC Software Laboratory Ningbo University Ningbo, Zhejiang 315211, China

Abstract: In this study, a method of using the watermark to enhance the security of the data hiding is proposed for H.264/AVC. The DCT coefficients in Intra-frames are modified to embed the watermark while the secrete information is inserted by modulating the appropriate MVD in P and B frames. The introduced Intra-watermarking, on one hand, can authenticate the integrity of the video stream. Furthermore, by the detected Intra-watermark and its integrity, the receiver can determine the reliability of the extracted hided information and judge whether the video has suffered from various attacks in addition, the security of the secrete communication can be guaranteed. Experiment results demonstrate that this scheme can achieve a large hiding capacity with low bit-rate increase, while the real-time performance can also be obtained.

Key words: H.264/AVC, video watermark, DCT, large capacity, motion vector, information hiding

INTRODUCTION

Video information hiding, as a secret communication technique, has become a new field of multi-media information security (Sang *et al*., 2009). The main idea is to embed a secret signal into a public video cover such that the signal in the marked video is imperceptible to the human eye, but can be extracted by a specific or corresponding detector, in this way the secret communication can be realized (Yang *et al*., 2011), (Wang *et al*., 2010; Mansouri *et al*., 2010). Qureshi and Tao (2006) has made a detail description about watermark. The key of information hiding is concluded as follows: (1) the scheme should balance the transparency, hiding capacity and payload, which are three conflicting aspects (Wang *et al*., 2009). (2) security of the secret information (Sang *et al*., 2009; Mansouri *et al*., 2010), the marked video should has little differences from the original to distract the attackers, in the mean while, the scheme must have the ability of judging whether the detected secret information is reliable or not, so as to avoid the wrong message to be read by the receiver.

The research about watermarking are focused on the image area in the early years (Zhang *et al*., 2010a; Zeng and Wu, 2010; Lv and Lu, 2011), fewer watermarking schemes are based on the encoded video, which is highly desirable.

H.264 as the most efficient and the latest compression standard is utilized in a wide range of application, therefore, providing a secure information hiding method, which is appropriate for this standard, is highly desirable (Mansouri *et al*., 2010). However, H.264 uses some new features such as Intra-prediction, variable block size and quarter-pixel motion estimation and compensation to improve the compression efficiency, these new features bring great challenges for data hiding because of less redundancy existed in the coded video stream. Existing video data hiding algorithm are all focus on the characteristics generated by the compression standard, in general, the data hiding for H.264 can be summarized into the following three aspects.

The works of the first category modulate the DCT coefficients and prediction mode of Intra-frame to embed information (Hu *et al*., 2008; Xu *et al*., 2010). (Zhang *et al*., 2010b). In study of Noorkami and Mersereau (2007) and Kim *et al*. (2009), information are inserted into DCT coefficients which can resist some common attacks, but the bit-rate would be increase sufficiently, furthermore, the hiding capacity is limited because of the number of I-frame is less. The authors in works (Yang *et al*., 2011; Wang *et al*., 2010; Hu *et al*., 2008) utilizes the intra-prediction-mode to hide information, the transparency is desirable, but these schemes can't resist any attacks, some common operation followed by re-encoding will make the information undetectable, therefore, the extracted secret information is distrustfully, the security issue is the major problem in this category (Mansouri *et al*., 2010). Mansouri *et al*. (2010) proposed a method that generates a public key from the Intra-mode to assign the hiding location which can increase the security, but the hiding capacity is limited make the scheme unpractical.

The second category of approaches inserts the information in motion vectors in P and B frames (Zheng *et al*., 2008; Kuo and Lo, 2009). Zheng *et al*. (2008) modulated the search range during the

Corresponding Author: Lujian Hu, CKC Software Laboratory Ningbo University Ningbo, Zhejiang 315211, China

motion estimation process to hide information can achieve a low bit-rate increase, but the hided information would affect the video quality sufficiently, in addition, the capacity is ignored. Kuo and Lo (2009) modified appropriate MV to embed the authentication watermark can get a desirable vulnerability, but these schemes can't resist any attacks and the bit-rate is ignored as well. One common attribute of the approaches of this type is very frail and can be utilized to realize the fragile watermarking, otherwise, the bit-rate would be affected to some extent in these schemes.

The schemes of the third category insert the information by modulating the VLC or CABAC bit-stream during the entropy-coding process (Zou and Bloom, 2009; Zou and Bloom, 2010; Seo and Choi, 2008). Zou and Bloom (2009) proposed a method that modified the code-word of the I4-mode to hide information, which would affect the video quality sufficiently because of he rate-distortion is ignored. In study of Zou and Bloom (2010), the appropriate MVD which have a bigger amplitude in P and B frames are selected and their CABAC code-word are modified to insert information, the capacity is limited because of the MVD is statistically lower which make the scheme unpractical. One advantage of these schemes is that the information can be detected just by partly decoded, thus, the computational complexity is low, however, both and video quality and the bit-rate would be affected to some extent because of the ignoring of the rate-distortion.

In this study, a large capacity of data hiding algorithm is proposed for H.264/AVC, with lower bit-rate achieved, furthermore, the intra-watermark is embedded into the video to increase the security. By the detected intra-watermark and its integrity, the receiver can determine the reliability of the extracted hided information and judge whether the video has suffered from various attacks in addition. The intra-watermark is realized by modifying the DCT coefficients in I-frames while the secret information is inserted by replacing the appropriate MVD in P and B frames.

Proposed method: In H.264/AVC, each frame is encoded in intra or inter mode, in the encoder, lots of elements would be produced, such as DCT coefficients, motion vector difference, prediction mode, etc. Information hiding is usually select such element and adjust them regularly according to a signal called secret information, the receiver could extract the secret information by a specific detector. The main idea of this study is to embed intra-watermark in the video which has included the hided information to authenticate the integrity of the video stream and then enhance the security in addition.

Statistical of residual coefficient and intra-watermark embedding:

- Distribution of I4 and I16 and statistics of the transfer probability after re-encoding

For the luminance samples in intra-frame, I4 or I16 encode mode would be selected for each macroblock. Actually, I16 is selected for smooth regions while I4 is appropriate for the more textured area (Mansouri *et al*., 2010), therefore, embed the watermark in I4 macroblock can get the transparency perfectly because of human eye is less sensitive to the textured area. As a matter of fact, after any simple processing followed by re-encoding, some macroblocks would change between I4 and I16, which will cause desynchronization during watermark extraction. in the experiment, the standard video sequences of foreman, container, carphone, news are re-encoded and then statistic their first fifteen intra-frames, the distribution of I4 and I16 and their transfer probability are shown in Table 1.

- Investigate of I4 prediction mode changes after re-encoding

After re-encoding, not only the encode mode would change between I4 and I16, other elements such as the prediction mode and the DCT would change as well. To estimate the characteristic, The distribution of I4 from various video sequences are counted according to their number of non-zero-coefficient (NNZ), furthermore, the prediction modes are sorted into 2 groups {0, 3, 4, 5, 7} and {1, 2, 6, 8} according to their directions (Mansouri *et al*., 2010), then calculate the intra-prediction mode change before and after classification, the NNZ value is given. The distribution and the change probability of I4 are shown in Fig. 1, the abscissa is the list of various values of NNZ. Form Fig. 1 we can find that the bigger the NNZ, the lower the change probability of

Table 1: Distribution of I4 and I16 and their transfer probability

	I4 (%)	I16 (%)	Changes of I4 and I16 (%)	Changes of I4 to I16 (%)
Foreman	94	6	4	3
Container	60	40	1	2
Carphone	84	16	4	4
News	86	14	2	2

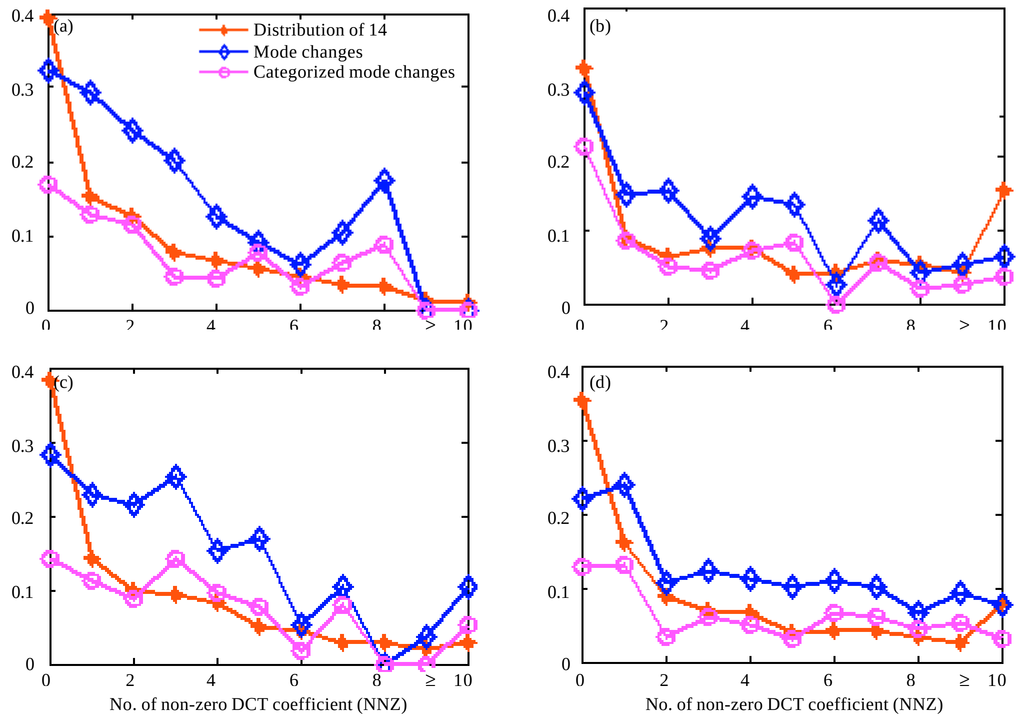


Fig. 1: Distribution of I4 and the probability of changes after re-encoding, (a) Foreman, (b) Container (c) Carphone and (d) News

Table 2: Changes of NNZ and prediction mode in I4 after re-encoding

	Foreman	Container	Carphone	News
Probability of the mode changes	0.1174	0.1002	0.1078	0.0890
Probability of the NNZ changes	0.0431	0.0463	0.0523	0.0365

the prediction mode and that after classification the conversion rate between two groups is lower than the original. In general, the encoder uses the rate-distortion-model which based on the algorithm of Lagrangian optimization to select the optimal prediction mode for each block, the optimal mode is denoted as m, in works (Yang *et al*., 2011; Mansouri *et al*., 2010; Hu *et al*., 2008) the authors modified the prediction mode to m' which is prior to m to hide information, this method can achieve the acceptable video quality consequently, however, after decompress and re-encoding, the encoder would select the optimal mode m but the m' according to the rate-distortion-model, this make the information undetectable.

- Changes of non-zero-coefficient and prediction mode in I4 after re-encoding

In order to explorer the attribute which can resist re-encoding more effectively, the rate of changes for the NNZ and prediction-mode in I4 are investigated after re-encoding. Firstly the I4 prediction modes are categorized into two groups as {0, 3, 4, 5, 7} and {1, 2, 6, 8}, then classified the NNZ value into two groups either as {0, 1, 2, 5, 6, 9, 10, 13, 14} and {3, 4, 7, 8, 11, 12, 15, 16}, the Statistical result of change is depicted in Table 2.

From Table 2 we can find that NNZ is more robust than prediction mode, moreover, watermarked prediction mode m' would changes to the optimal mode m after re-encoding and the NNZ does not happen, consequently, NNZ is robust to re-encoding enough and we can utilize this to embed the intra-watermark.

- Intra-watermark embedding

In order to prevent desynchronization, most of the relative works aim at selecting the more steady blocks to hide information, however, transfer problem still exits more or less, only one watermarked-macrolbock changes would cause desynchronization and make the detection fail. In this case, this paper propose a method that embed watermark in every macroblock in intra-frames, that means,

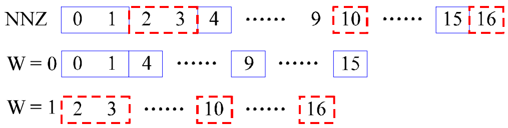


Fig. 2: The categorization scheme of NNZ and intra-watermark embedding

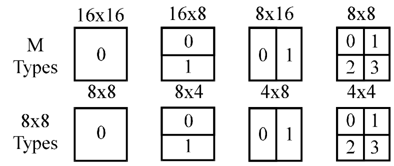


Fig. 3: Macroblock partitions

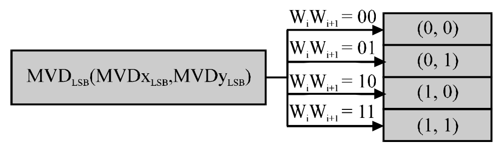


Fig. 4: Modulate MVD_{LSB} hiding data

each intra-macroblock is correspond to one bit, in the decoder, the watermark can be extracted bit to bit from every macroblock in intra-frames. In this way the synchronization problem can be solved.

Every macroblock in I-frames are embed in 1 bit orderly to realize the intra-watermark. In I4, firstly the NNZ is categorized into 2 groups, as shown in Fig. 2, here the scheme of categorization can be various and make it as the private key to extract the watermark in the detector, this is one of the measures to enhance the security, furthermore, the target 4×4 block which has the biggest NNZ value in the current I4 is selected, which category the NNZ of the block belongs to indicates the watermark bit, therefore, the higher-frequency zero-DCT-coefficient is set to 1 to satisfy the condition. The higher-frequency DCT coefficient is selected to achieve controllable video quality, this scheme embed the watermark by set the zero-coefficient to 1 but clear the zero-coefficient to ensure that after watermark embedding the NNZ value of the 4×4 block is still the biggest one, the very block can be located by this condition and detect the watermark implicitly in the receiver.

I16 contributes a small part in I-frames, watermark in I16 is embed to prevent desynchronization and this scheme modulate the DC coefficient of luma samples in the current I16 to embed watermark, as depicted in Eq 1.

$$\mathrm{DC(LSB)}{+}{=}1 \quad \mathrm{if}(W_i != \mathrm{DC(LSB)}) \tag{1}$$

The watermark, which is embedded in every macroblock in I-frames, is robust enough to resist re-encoding and can be utilized to authenticate the integrity of the video stream, furthermore, the watermark can be used to detect whether the video has suffered from re-encoding and determine the reliability of the secret information.

Motion vector and information hiding: H.264 CODEC uses the method of block-based motion estimation and motion compensation, after a tree structured partition the macroblocks is divided into several sizes, which is ranging from 16×16 to 4×4, as depicted in Fig. 3. The AVC encoder selects the best partition size for each part of the frame, separate motion estimation and compensation is required for each partition or sub-partition, in general, a large partition size is appropriate for static-area of the frame and a small partition size may be beneficial for the motion areas. In the mean while, the small partitions need more motion information and can utilize it to hide more information.

Encoding a motion vector for each partition can take a significant number of bits, especially if small partition sizes are chosen. In order to decrease the redundancy of the correlation among neighboring partitions, the AVC CODEC calculate the prediction vector MVp based on the previously calculated motion vectors of neighboring, the difference motion vector between MV and MVp is encoded and transmitted finally. The motion vector difference MVD including two direction components formed as (MVDx,MVDy), in this study, this scheme insert the information before the entropy-coding process, the scheme is described as follows:

- **Step 1:** The MVD, which satisfied the condition of $|MVDx|\geq 2$ or $|MVDy|\geq 2$, are selected and added to the embedding aggregate S

$$S = \{MVD1, MVD2, \ldots, MVDn\}$$

- **Step 2:** Take every MVD in the aggregate S through a binary processor, then the LSB bit of its x and y components can formed as $MVD_{LSB}(MVDx_{LSB}, MVDy_{LSB})$. Set or cleared each MVD_{LSB} to data 2 bits information, as shown in Fig. 4.

The MVD which can hiding information satisfy the condition of $|MVDx|\geq 2$ or $|MVDy|\geq 2$. Modify the LSB of MVD to perform data insertion. If the original MVD_{LSB} is (1,1), it will be modified to one of the four cases (0, 0),(0, 1),(1, 0) or (1, 1)after data hiding process. It is shown in Fig. 5.

It has high capacity by modifying MVD which can embed 2 bits information with little impact on video quality. In fact, the being modified magnitude of MVD is $0 \le |d_{MVD}| \le \sqrt{2}$. After data hiding, the MVD still satisfy the condition of $|MVDx| \ge 2$ or $|MVDy| \ge 2$,, according to which the embedded aggregate S'_w can be obtained, $S'_w = \{MVD1_w, MVD2_w, \ldots, MVDn_w\}$, then the embedded information can be extracted.

Data extraction: This scheme could extract the watermark quickly and simply and do not need the original video stream for reference. The intra-watermark can be detected from the DCT coefficient in I-frames while the secret information can be extracted by partly decode the MVD data. More details about the extraction are described as follows.

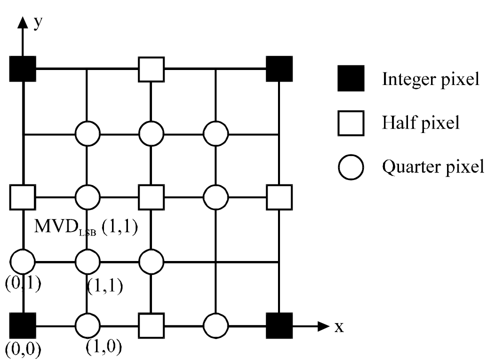


Fig. 5: Changes of MVD after hiding data

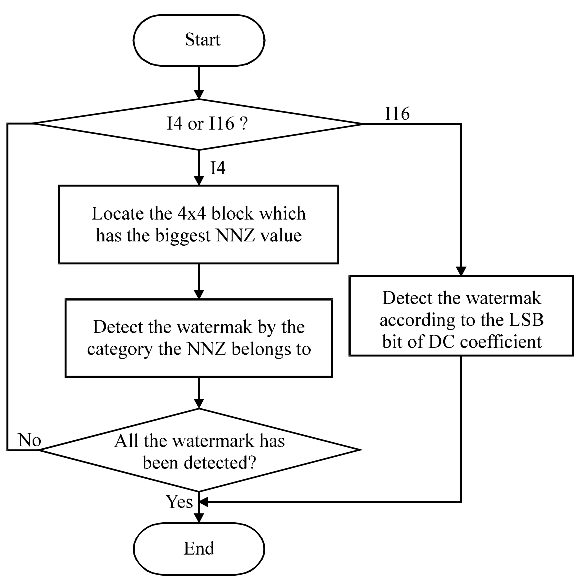


Fig. 6: Intra-watermark detection

Intra-watermark extraction: Detect the intra-watermark orderly from the macroblocks in I-frames, as depicted in Fig. 6. this scheme use different methods to extract watermark from I4 and I16. In I4, firstly the detector locates the 4×4 block which has the biggest NNZ, which category the NNZ belongs to indicate the watermark, as depicted in Fig. 2,. In I16, the watermark can be detected just by reading the LSB bit of the DC coefficient, as shown in Eq. 2.

$$W_i = DC_{LSB} \tag{2}$$

Secret information detection: The MVD which include secret information satisfy the condition of $|MVDx| \ge 2$ or $|MVDy| \ge 2$, according to which the hiding aggregate S'_w can be obtained.

$$S'_w = \{MVD1_w, MVD2_w, \ldots, MVDn_w\}$$

Extract the hiding information from elements of S'_w, take each of them through a binary processor, then read the LSB bit of its x and y components to form 2 bit hiding information, as shown in Eq. 3.

$$\begin{aligned} W_i &= MVDx_{LSB} \\ W_{i+1} &= MVDy_{LSB} \end{aligned} \tag{3}$$

Read every MVD from S'_w orderly until the hiding data have been detected completely.

EXPERIMENT PERFORMANCE AND ANALYSIS

In order to verify the performance and effectiveness of our proposed hiding algorithm, we implemented our method using the H.264 reference software version JM8.6 (Suehring, 2010) using the following 8 QCIF format standard video sequences: foreman, carphone, container, news, bridge-close, highway, mother-daughter, silent. All videos are coded at 15 frames/s with "IBPBP..." GOP structure, main profile are adopted, 75 frames are coded in total. The hided information is a binary random sequence, the intra-watermark is a 34×43 binary image, as shown in Fig. 7.

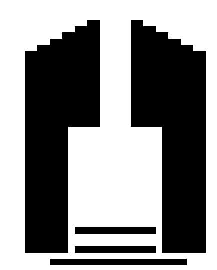


Fig. 7: Intra-watermark image

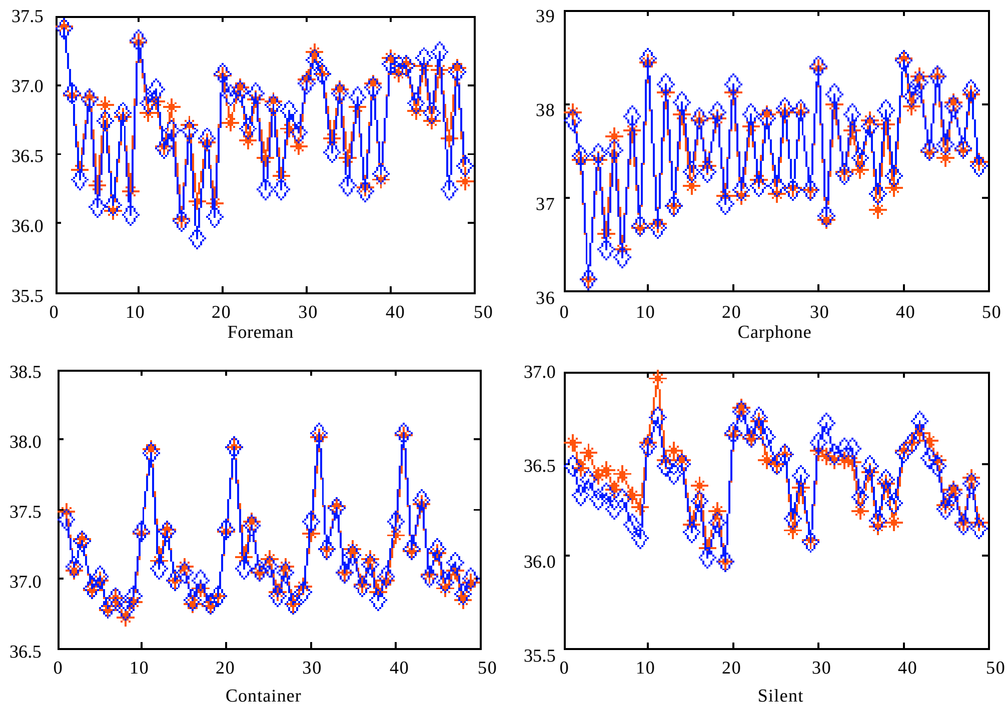


Fig. 8: PSNR comparison

Table 3: Performance comparison

	This paper		literature (Hu *et al.*, 2008) (1/8-b)		literature (Xu *et al.*,2010) (n = 2)	
	(%)	(bit)	(%)	(bit)	(%)	(bit)
Foreman	0.2	18738	0.9	1642	0.16	1991
Carphone	0.3	12004	1	1199	0.19	1482
Container	0.7	1702	0.3	1003	0.17	755
News	0.2	7112	0.25	1246	0.14	1291
Bridge-close	0.3	3426	0.51	1697	0.1	1709
Mother-daughter	0.8	5610	0.5	1138	0.27	1175
Silent	0.3	7700	0.07	2231	0.11	2425
Highway	0.4	9380	0.5	1100	0.48	1101

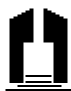
Experiment performance: Figure 8 illustrates the PSNR comparison of the first 5 GOP between the original and the data hided video of foreman, carphone, container and silent. From which we can find that the data hiding introduces little influence to the video. The main reason can be concluded into the following 2 aspects: (1) We modulate the higher-frequency DCT coefficient to embed the intra-watermark, in addition, we adjust the embed strength to achieve the controllable video quality. (2) We modulate the LSB bit of appropriate MVD to perform data hiding, the change of the magnitude is $0 \le |d_{MVD}| \le \sqrt{2}$, which has little effect on the video quality; furthermore, only a certain range of the motion vectors will be selected to embed the data refer to the HVS(human visual system), so the subjective video quality is ensured. We compared the data hided video with the original to evaluate the imperceptible performance subjectively, Figure 9 displays the I, P and B frames of foreman before and after data insertion, there are little difference between the watermarked image and the original, so the algorithm meet the human perceptual requirement.

The increasing percentage in video for bit-rate μ is introduced to estimate the performance of the algorithm in addition.

$$\mu = \frac{m-u}{u} \times 100\% \tag{4}$$

where, m and u denotes the bit-rate of the data hided video and the original respectively, the hiding capacity C, as one of the important parameter of hiding scheme, denotes the number of bits of data hiding. We display the parameters of μ and C of the algorithm and compared them with literature Hu *et al.* (2008) and Xu *et al.* (2010), as shown in Table 3.

Table 4: Intra-watermark detection under various conditions

		Attacks		
	Without attacks	Re-encoding	Median filtering	Mirror transformation
Foreman	*h* =100	*h* =85.6	*h* =52.5	*h* =50.7
				
Carphone		*h* =81.9	*h* =53.8	*h* =52.4
				
Container		*h* =80.2	*h* =53.8	*h* =49.8
				
News		*h* =86.2	*h* =51.2	*h* =50.6
				
Bridge-close		*h* =80.0	*h* =52.5	*h* =48.1
				
Mother-daughter		*h* =76.7	*h* =52.1	*h* =47.3
				
Silent		*h* =84.8	*h* =48.2	*h* =50.4
				
Highway		*h* =68.6	*h* =52.1	*h* =52.0
				

From Table 1 we can find that the hiding scheme has an improvement compared with previous, We select the appropriate MVD data which satisfy the condition of $|MVDx|\geq 2$ and $|MVDy|\geq 2$ to implement data hiding, the data is inserted by modifying the LSB bit of its x and y components, so the bit-rate is desirable, furthermore, we modify every MVD inserting 2 bits, therefore, the large hiding capacity can be achieved. Meanwhile, from Table 3, we can also find that the embedding capacity is decided by the motion complexity of the video itself, a bigger capacity could be achieved in the higher motion video such as foreman, carphone, for lower motion video such as container and bridge-close, the capacity is smaller.

Security: In this study, intra-watermark is introduced to enhance the security of the information hiding algorithm. By the detected intra-watermark and its integrity, the receiver can determine the reliability of the extracted hided information and judge whether the video has suffered from various attacks in addition. The experiment attack our video under re-encoding, median filtering and image transformation to test whether the intra-watermark can verify the integrity of video content or not and introduce a recovery rate η to evaluate the performance, as shown in Eq. 5.

$$\eta = \frac{\text{recovered pixels}}{\text{total pixels}} = \frac{\sum_{j=1}^{N}\sum_{i=1}^{M} W(i,j)W'(i,j)}{M\times N}\times 100\% \tag{5}$$

where, M and N denotes the width and height of the watermark image respectively, W denotes the original watermark while W' denotes the extracted one.

Table 4 depicted the extraction, from which we can find that the intra-watermark can be detected fully

Fig. 9: Frames before and after data hiding

with no attacks, meanwhile, the detected intra-watermark can be recognized and can resist the re-encoding effectively after re-encoding, after median filtering and image transformation followed by re-encoding, the intra-watermark can't be recognized any more. Therefore, the characteristic of the intra-watermark can be utilized to detect whether the video has been suffered from various attacks, if the intra-watermark can be extracted fully we can determine that the video is integrated and the secret is reliable, otherwise, if the extracted intra-watermark is fragmentary we can judge that the video has been attacked and the secret information is untrustworthy.

CONCLUSIONS

This study proposed a method of utilizing the intra-watermark to enhance the security of the information hiding algorithm. the scheme modulate the MVD in P and B frames to insert the secret information and modify the higher-frequency DCT coefficient of in I-frames to embed the intra-watermark, in I-frames, every macroblock is embed in 1 bit watermark orderly to prevent desynchronization. The intra-watermark is introduced to authenticate the integrity of the video stream and enhance the security of the information hiding algorithm furthermore. The hiding and extraction processes can perform quickly, simply, which satisfy the need of real-time signal processing.

ACKNOWLEDGMENTS

This study is supported by the National Natural Science Foundation of China under Grant No. 60873220, Zhejiang Natural Science Foundation under Grant No.Y1090285, Ningbo Natural Science Foundation under Grant No. 2009A610085 and No.2010A610110, Ningbo Science and Technology Project under Grant No. 2009B10003.

REFERENCES

Hu, Y., C.T. Zhang and Y.T. Shu, 2008. Information hiding for H.264/AVC. Acta Electronica Sinica, 36: 690-694.

Kim, W.J., J.K. Lee, J.H. Kim and K.R. Kwon, 2009. Block-based watermarking using random position key. Int. J. Comput. Sci. Network Secur., 9: 83-87.

Kuo, T.Y. and Y.C. Lo, 2009. Fragile video watermarking technique by motion field embedding with rate-distortion minimization. J. Commun. Comput., 6: 16-23.

Lv, M.L. and Z.M. Lu, 2011. Multipurpose perceptual image hashing based on block truncation coding. Inform. Technol. J., 10: 207-212.

Mansouri, A., A.M. Aznaveh, F. Torkamani-Azar and F. Kurugollu, 2010. A low complexity video watermarking in H.264 compressed domain. IEEE Trans. Inform. Forens. Secur.,, 5: 649-657.

Noorkami, M. and R.M. Mersereau, 2007. A framework for robust watermarking of H.264-encoded video with controllable detection performance. IEEE Trans. Inform. Forens. Secur., 2: 14-23.

Qureshi, M.A. and R. Tao, 2006. A comprehensive analysis of digital watermarking. Inform. Technol. J., 5: 471-475.

Sang, J., H. Xiang. N. Sang and L. Fu, 2009. Increasing the data hiding capacity and improving the security of a double-random phase-encoding technique based information hiding scheme. Opt. Commun., 282: 2713-2721.

Seo, Y.H. and H.J. Choi, 2008. Low-complexity watermarking based on entropy coding in H.264 AVC. Inform. Community Eng., E91: 2130-2137.

Suehring, K., 2010. H.264/AVC JM Reference Software. http://iphome.hhi.de/suehring/tml/download/.

Wang, Y.G., Z.M. Lu, F. Liang and Y. Zheng, 2009. Robust dual watermarking algorithm for AVS video. Signal Process. Image Commun., 24: 333-344.

Wang, R., H. Zhu and D. Xu, 2010. Information hiding algorithm for H.264/AVC based on encoding mode. Opto-Electron. Eng., 37: 144-150.

Xu, D., R. Wang and J. Wang, 2010. Prediction mode modulated data-hiding algorithm for H.264/AVC. J. Real-Time Image Proc., 10.

Yang, G., J. Li, Y. He and Z. Kang, 2011. An information hiding algorithm based on intra-prediction modes and matrix coding for H.264/AVC video stream. AEu Int. J. Electron. Commun., 65: 331-337.

Zeng, W. and Y. Wu, 2010. A visible watermarking scheme in spatial domain using HVS model. Inform. Technol. J., 9: 1622-1628.

Zhang, Y., Z.M. Lu and D.N. Zhao, 2010a. A blind image watermarking scheme using fast hadamard transform. Inform. Technol. J., 9: 1369-1375.

Zhang, Y., Z.M. Lu and D.N. Zhao, 2010b. Quantization based semi-fragile watermarking scheme for H.264 video. Inform. Technol. J., 9: 1476-1482.

Zheng, Z.D., P. Wang and S. Cheng, 2008. A video watermarking scheme based on the region character of motion vectors. J. Image Graph., 10: 1926-1929.

Zou, D. and J.A. Bloom, 2009. H.264/AVC substitution watermarking: A CAVLC example. Proceedings of the SPIE Media Forensics and Security Symposium, January 19, 2009, San Jose, CA, USA.

Zou, D. and J.A. Bloom, 2010. H.264 stream replacement watermarking with CABAC encoding. Proceedings of the IEEE International Conference on Multimedia and Expo, July 19-23, 2010, Suntec City, pp: 117-121.