International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:5, No:6, 2011

Post-Compression Consideration in Video Watermarking for Wireless Communication

Chuen-Ching Wang, Yao-Tang Chang and Yu-Chang Hsu

***Abstract*—**A simple but effective digital watermarking scheme utilizing a context adaptive variable length coding (CAVLC) method is presented for wireless communication system. In the proposed approach, the watermark bits are embedded in the final non-zero quantized coefficient of each DCT block, thereby yielding a potential reduction in the length of the coded block. As a result, the watermarking scheme not only provides the means to check the authenticity and integrity of the video stream, but also improves the compression ratio and therefore reduces both the transmission time and the storage space requirements of the coded video sequence. The results confirm that the proposed scheme enables the detection of malicious tampering attacks and reduces the size of the coded H.264 file. Therefore, the current study is feasible to apply in the video applications of wireless communication such as 3G system

***Keywords*—**3G, wireless communication, CAVLC, digital watermarking, motion compensation

I. Introduction

DUE to the widespread proliferation of digital video applications and the ready availability of ever more powerful digital duplication / manipulation tools, there is an urgent need for sophisticated schemes capable of verifying the integrity of video streams transferred over communication networks such as the Internet. This requirement is often satisfied by using a fragile watermarking scheme to detect the occurrence of malicious tampering attacks and to pinpoint the location within the video stream at which such attacks occur [1-5]. Traditional fragile watermarking schemes are designed to satisfy three basic criteria, namely (1) perceptual transparency, (2) a high sensitivity to tampering attacks, and (3) the ability to detect changes in the streamed content without reference to the original content. Bartolini et al. [1] embedded the watermark bits in the quantized coefficients of each DCT block in accordance with a predefined threshold such that the coefficients in an even position in the zigzag reordering assumed an even value, while those in an odd position assumed an odd value. Zhou et al. [3] proposed a fragile watermarking scheme in which the values of all the quantized DCT coefficients in each 8×8 DCT block after a certain zigzag scan position were modified to a small even value equal to that of the nearby coefficients. In the extraction process, the watermarked coefficients in each DCT block were inspected, and a non-even coefficient value was taken as evidence of channel errors or a tampering attack. Lie et al. [5] embedded the watermark information in the I- and P-frames of the coded video stream using a LSB replacement scheme. In the I-frame, the watermark data was embedded in the quantized dc coefficients corresponding to the two LSBs using the direct replacement method, while in the P-frame, the watermark data was embedded in selected ac coefficients (e.g., the first and second coefficients in the zigzag scanning order) using the modulo 2 method. However, whilst the fragile watermarking schemes described above all satisfy the three basic design criteria to a greater or lesser extent, the effect of the watermark information on the bit rate of the coded content was not discussed.

To resolve the limitations of the watermarking schemes described above, the current study develops a fragile watermarking algorithm in which the watermark bits are embedded in the last non-zero coefficient within each DCT block of the I- and P-frames of the H.264 video stream during the CAVLC encoding process [6]. Since the watermark information is deliberately embedded within the final non-zero coefficient in the DCT block, and a finite possibility exists that the embedding process causes the value of this coefficient to be modulated to "0", the proposed scheme has the potential to reduce the length of the coded block. As a result, the watermarking algorithm enhances the compression rate of the video stream, thereby reducing both the transmission time and the storage space requirements of the coded video.

The remainder of this paper is organized as follows. Section II describes the watermark embedding process and the corresponding post-compression effect. Section III presents the results of a series of experimental simulations designed to verify the effectiveness of the proposed scheme. The proposed communication architecture is described in Section IV. Finally, Section V provides some brief concluding remarks.

II. Watermark Embedding and Post-Compression Effect

A. Previous Work

In a previous study [7], the present group proposed a watermarking method for the authentication of H.264 video

[A] Chuen-Ching Wang, Department of Information Management, Shu-Zen College of Medicine and Management, Taiwan (ccwang@ms.szmc.edu.tw).
[B] Yao-Tang Chang, Department of Electro-Optical Science and Engineering, Kao Yuan University, Taiwan (t10066@cc.kyu.edu.tw)
[C] Yu-Chang Hsu, Department of Electrical Engineering, National Chang-Hua University, Taiwan (imsend@yahoo.com.tw).

content in which the value of the last non-zero coefficient in each DCT block was modified to an odd or even number depending on the value of the watermark bit. The proposed scheme utilized the following 4×4 DCT transformations [11]:

$$Y = AXA^T \quad (1)$$

where X is the raw-data matrix, Y is the matrix of the corresponding DCT coefficients, and A is a 4×4 transform matrix with the form

$$A = \begin{vmatrix} a & a & a & a \\ b & c & c & b \\ a & a & a & a \\ c & b & b & c \end{vmatrix} \quad (2)$$

where a =1 /2 , b = $1/\sqrt{2}\cos(\pi/8)$, and c = $1/\sqrt{2}\cos(3\pi/8)$.

The scheme proposed in [7] inserts a watermark bit ϖ at a specific location within each quantized DCT block q. The embedding point is determined using an adaptive selection strategy which satisfies the requirements for size reduction, perceptual transparency and sensitivity to tampering attacks by specifically choosing the final non-zero coefficient in q (as identified in a zigzag scan). Let φ denote the selected DCT coefficient. The watermarked block, q^w , is obtained by modulating φ to $\overline{\varphi}$ in accordance with the following rule:

$$\overline{\varphi} = \begin{cases} sign(\varphi)(|\varphi| - 1) & if\ \varpi \oplus E(\lambda) = 0 \\ \varphi & if\ \varpi \oplus E(\lambda) = 1 \end{cases} \quad (3)$$

where sign(φ) indicates the sign of φ (i.e. positive or negative) and $|\varphi|$ denotes the absolute value of φ . Furthermore, E (λ) = (λ +1) mod 2 and λ is the number of odd value coefficients in q.

B. Proposed Watermarking Scheme

In the present study, the watermarking scheme proposed in [7] is extended to improve the compression efficiency at the sender end. The basic structure of the proposed scheme is illustrated in Figure 1. As shown, the coding process commences by using a quantization procedure to reduce the value of the DCT coefficients in order to enhance the compression of the video stream. The video encoder then embeds a fragile watermark into the quantized DCT coefficients before they are processed by the CAVLC scheme. Note that the watermark information is deliberately embedded in the quantized DCT block rather than the non-quantized DCT block since the quantization process would destroy the embedded watermark information and prevent its extraction in the subsequent decoding process. As described in the previous section, the watermarking scheme proposed in [7] embeds the watermark information by modulating the last non-zero coefficient in each DCT block to an even or odd number depending on the value of the watermark bit (see Eq. (3)). However, in the present study, the watermarking scheme proposed in [7] is modified such that the last non-zero coefficient in each 4 × 4 DCT block is either modulated to zero or is unchanged in accordance with the following formulation:

$$\overline{\varphi} = \begin{cases} 0 & if\ \varpi \oplus E(\lambda) = 0 \\ \varphi & if\ \varpi \oplus E(\lambda) = 1 \end{cases} \quad (4)$$

On the decoder side, the watermarked bits, ϖ' , are detected in accordance with

$$\varpi' = \begin{cases} 0 & if\ \ E(\overline{\lambda}) = 1 \\ 1 & if\ \ E(\overline{\lambda}) = 0 \end{cases} \quad (5)$$

where $E(\overline{\lambda})$ = ($\overline{\lambda}$ +1) mod 2 and $\overline{\lambda}$ is the number of odd value coefficients in the 4 x 4 DCT watermarked block.

In Eq. (5), a value of ϖ' not equal to ϖ indicates that the original 4×4 DCT block has been corrupted in some way, e.g. by channel errors or tampering attacks. As a result, the watermarking scheme provides the means to authenticate the content of the received video stream and to pinpoint the location of any changes in the original content. Furthermore, in Eq. (4), there is a finite possibility that the value of the last non-zero coefficient in each 4×4 DCT block will be modulated to zero. In other words, the watermark embedding process has the potential to reduce the number of encoded symbols, thereby reducing the length of the CAVLC-encoded block. As a result, the watermarking scheme not only provides a content authentication capability, but also yields a post-compression effect, thereby reducing the storage space requirements of the encoded H.264 video sequence and improving the transmission time.

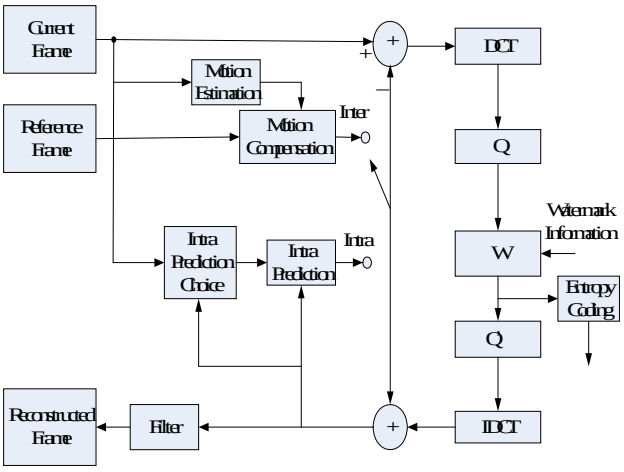

Fig. 1 Structure of H.264 video encoder utilizing proposed watermarking technique

C. Post-Compression Illustration

In this section, the post-compression feature of the proposed watermarking scheme is illustrated using a simple example. As described in [6], the basic steps in the CAVLC encoding of a block of transform coefficients are as follows:

1) Encode the number of coefficients and trailing ones;

2) Encode the sign of each trailing one;
3) Encode the levels of the remaining non-zero coefficients;
4)Encode the total number of zeros before the last coefficient;
5) Encode each run of zeros.

Consider the following I-frame residual 4 ×4 block (Refer Fig. 2):

The zigzag re-ordering of this block has the form: 0,3,0,1,-1,-1,0,1,0,0,1,0,0,0,0,0. Therefore, NumCoeff=6, TotZero=3, and T1s=3. (Note that NumCoeff is the number of non-zero coefficients in the residual 4×4 block, TotZero is the number of zeros after the non-zero coefficient in the residual4×4 block, and T1s is the number of trailing ones in the residual 4 ×4 block.) In accordance with the H.264 coding standard, the zigzag re-ordering of the block is encoded as follows (see Table 1):

0	3	-1	0
0	-1	1	0
1	0	0	0
0	1	0	0

Fig. 2The quantized block of H.264

TABLE 1
THE CORRESPONDING CAVLC CODE FOR FIGURE II

Value	Code	Comments
NumCoeff=6, T1s=3	00010101	Use Num-VLC0
sign of T1 (1)	0	Starting at highest frequency
sign of T1(1)	0	
sign of T1(-1)	1	
Level= -1	01	Use Lev-VLC0
Level= 1	10	Use Lev-VLC1
Level= 2	0010	Use Lev-VLC1
TotZeros=3	000	Also depends on NumCoeff
ZerosLeft=3;RunBefore=2	11	RunBefore of the 1st Coeff
ZerosLeft=3;RunBefore=1	00	RunBefore of the 2nd Coeff
ZerosLeft=2;RunBefore=0	1	RunBefore of the 3rd Coeff
ZerosLeft=2;RunBefore=0	1	RunBefore of the 4th Coeff
ZerosLeft=2;RunBefore=1	01	RunBefore of the 5th Coeff
ZerosLeft=1;RunBefore=1		No code required; last coeff

Hence, the transmitted bit stream for the block has the form 000101010010110001000011001101. In other words, the block contains a total of 30 bits.

In the proposed watermarking scheme, the watermark is embedded within the H.264 video stream by modifying the last non-zero coefficient in each residual block. As described in the previous section, there is a finite probability that the final non-zero coefficient will be modified to zero. In other words, the block is modified as follows (see Fig. 3):

:

0	3	-1	0
0	-1	1	0
1	0	0	0
0	0	0	0

Fig. 3The quantized block of H.264

As shown in Table II, the modified block is then encoded as follows:

TABLE I
THE CORRESPONDING CAVLC CODE FOR FIGURE 3

Value	Code	Comments
NumCoeff=5, T1s=3	0001011	N=0 → Use Num-VLC0
sign of T1(1)	0	Starting at highest frequency
sign of T1(-1)	1	
sign of T1(-1)	1	
Level= 1	1	Inter frame → Use Lev-VLC0
Level =3	0010	Use Lev-VLC1
TotZeros=3	1110	Also depends on NumCoeff
ZerosLeft=3;RunBefore=1	00	RunBefore of the 1st Coeff
ZerosLeft=2;RunBefore=0	1	RunBefore of the 2nd Coeff
ZerosLeft=2;RunBefore=0	1	RunBefore of the 3rd Coeff
ZerosLeft=2;RunBefore=1	01	RunBefore of the 4th Coeff
ZerosLeft=1;RunBefore=1		No code required; last coeff

The transmitted bit stream therefore has the form 000101101110010111000 1101. In other words, the transmitted block contains a total of 25 bits. Thus, in contrast to the non-watermarked block, the size of the transmitted watermarked block is reduced by 5 bits. In other words, the post-compression ratio is around 16.6% for this particular DCT residual block and the post-compression benefit of the proposed scheme thus can be proved.

III. EXPERIMENTAL RESULTS

This section evaluates the performance of the proposed watermarking scheme in terms of three criteria, namely (1) the effect of the watermark information on the perceived video quality; (2) the sensitivity of the watermark to malicious attack, and (3) the compression rate improvement. The evaluation trials consider 14 standard video sequences. In conducting the simulations, the performance of the proposed watermarking

scheme is compared with that of two other watermarking schemes, namely Method 1: identical to that proposed in [7], but applied to the odd DCT residual blocks only; and Method 2: the method proposed in [7], applied to both odd and even DCT residual blocks.

A. Video Quality Degradation

The effect of the embedded watermark information on the visual quality of the video sequences was evaluated using the PSNR (peak signal-to-noise ratio) metric, defined as

$$PSNR(dB) = 10 \times \log \frac{255^2}{MSE} \tag{6}$$
$$MSE = (\frac{1}{M \times N}) \sum_{i=1}^{M} \sum_{j=1}^{N} [x(i, j) - \hat{x}(i, j)]^2$$

where *MSE* denotes the mean square error between the original image (x) and the reconstructed image ($\hat{x}$), and M and N are the length and width of the image in pixels, respectively. Note that the evaluation trials were performed using a quality parameter (QP) of QP=28. In addition, each video test sequence comprised a total of 120 frames.

Figure 4 compares the frame-by-frame PSNR values of the original Flower sequence with those of the sequences processed using the proposed watermarking scheme, the Method 1 scheme and the Method 2 scheme, respectively. The average PSNR values of the non-watermarked stream and the three watermarked streams are found to be as follows: 35.37dB, 34.25dB (proposed scheme), 34.91dB (Method 1) and 34.28dB (Method 2). It is observed that the video quality of the sequence processed using the Method 1 watermarking scheme is closer to that of the original (non-watermarked) sequence than that of the other two watermarked sequences. This result is to be expected since the Method 1 watermarking scheme results in fewer final non-zero coefficients in the DCT blocks being modified during the watermark embedding process (i.e. the scheme is applied to the odd DCT blocks only).

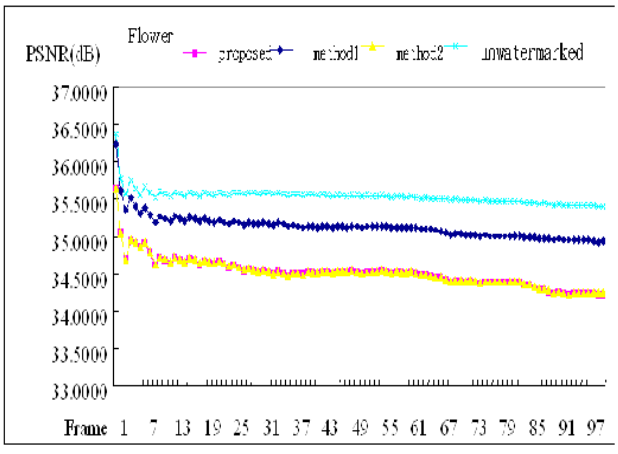

Fig. 4 Comparison of effects of three watermarking schemes on video quality. (Test sequence: Flower.)

respectively. The average PSNR values are found to be as follows: 35.02dB (non-watermarked), 32.95dB (proposed scheme), 34.19dB (Method 1) and 33.01dB (Method 2). As in the previous example, it is seen that the Method 1 watermarking scheme results in a better video quality than the proposed scheme or the Method 2 scheme since it results in the modification of fewer DCT coefficients. Table 3 summarizes the PSNR degradation of the three watermarking schemes for each of the 14 test video sequences.

B. Post-Compression Performance

As illustrated in Section 2.C, the proposed watermarking scheme has the potential to reduce the length of the CAVLC encoded blocks since there is a finite possibility that the last non-zero coefficient in each 4×4 DCT block will be modulated

TABLE III
PSNR PERFORMANCE COMPARISON OF THREE WATERMARKING SCHEMES

Video \ Method	Method 1 PSNR loss (dB)	Proposed scheme PSNR loss(dB)	Method 2 PSNR loss(dB)
Akiyo	1.274	2.069	2.061
Bus	0.835	2.077	2.015
Coastguard	1.688	2.799	2.775
Container	0.648	1.391	1.379
Flower	0.455	1.114	1.089
Foreman	0.701	1.618	1.597
Hall	0.589	1.689	1.682
Mobile	0.391	1.103	1.066
Motherdaughter	1.740	2.633	2.621
News	0.431	2.369	2.366
Silent	1.656	3.284	3.272
Stefan	0.869	2.010	1.983
Tempete	0.631	1.511	1.431
Waterfall	1.268	2.155	2.143

to "0". In this section, the resulting coding efficiency gain is quantified using the following compression ratio improvement (CRI) metric:

$$CRI = \frac{S_N - S_W}{S_N} \times 100\% \tag{7}$$

where S_N and S_W are the file sizes of the non-watermarked video sequence and the watermarked video sequence, respectively.

Figures 5 shows the frame-by-frame CRI values of the Flower video sequences, respectively, when processed using the proposed watermarking scheme, the Method 1 watermarking scheme and the Method 2 watermarking scheme. The average CRI values for the Flower sequence are as follows: 3.92% (proposed scheme), 1.31% (Method 1), and 3.84% (Method 2). In other words, the post-compression performance of the proposed scheme is superior to that of the other watermarking schemes. Significantly, the CRI of the Method 1 watermarking scheme is around half that of the proposed scheme or the

Method 2 scheme since it considers only the odd DCT blocks rather than all the DCT blocks.

Table 4 compares the CRI performance of the three watermarking schemes for each of the 14 test video sequences. The average CRI value for the proposed are found to be as follows: 2.78% (proposed scheme), 1.18% (Method 1) and 2.75% (Method 2).

C. Sensitivity of Proposed Watermarking Scheme to Malicious Attack

If the watermarked image is not modified during transmission, the number of odd coefficients in each watermarked DCT block is unchanged, and thus the extracted watermark bit is identical to the embedded watermark bit. However, if the watermarked video is changed in some way following the encoding process, the change is immediately obvious in the watermark bitmaps extracted from the corresponding frames.

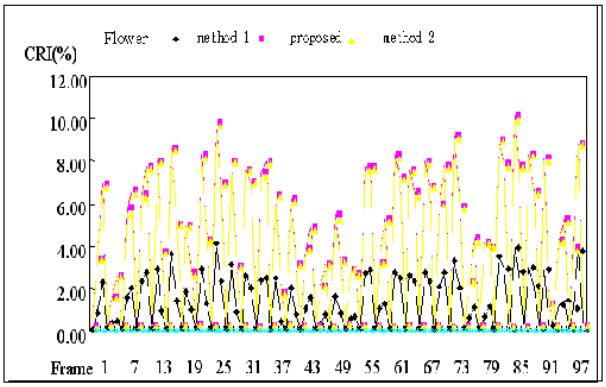

Fig. 5 CRI comparison for Flower video sequence

TABLE IV
. CRI PERFORMANCE COMPARISON OF THREE WATERMARKING SCHEMES

Video \ Method	Method 1 CRI	Proposed scheme CRI	Method 2 CRI
Akiyo	0.232%	0.800%	0.797%
Bus	1.611%	4.031%	3.991%
Coastguard	4.905%	8.400%	8.374%
Container	0.140%	0.402%	0.398%
Flower	1.318%	3.920%	3.846%
Foreman	0.777%	1.877%	1.865%
Hall	0.545%	1.651%	1.631%
Mobile	1.014%	3.197%	3.149%
Motherdaughter	0.979%	1.688%	1.679%
News	0.440%	1.561%	1.550%
Silent	0.766%	1.799%	1.792%
Stefan	1.574%	3.889%	3.854%
Tempete	1.439%	3.913%	3.879%
Waterfall	0.821%	1.736%	1.729%

Consider the scenario in which the watermarked Stefan video frames shown in Figure 6 are modified via the addition of the grid lines shown in Figure 7 such that it appears that the tennis game is held indoors whereas in fact it is actually held outdoors. Figures 8 and 9 show the extracted watermark bit maps for the original video sequence and the tampered video sequence, respectively. Comparing the two sets of bitmaps, it is evident that the bitmaps associated with Figure 7 contain significant distortion. Furthermore, it can be seen that the regions of distortion in Figure 9 coincide roughly with the tampered regions in Figure 7. In other words, the proposed watermarking scheme not only identifies those frames which have been illegally modified, but also indicates the tampering location within each frame. (Note that the sensitivity of the watermarking scheme to other forms of malicious attack, e.g. noise attacks, GOP replacement frame attacks, frame removal attacks, and so on, is documented in [7].)

Fig. 6 Watermarked Stefan video frames

Fig. 7 Tampered watermarked Stefan video frames.

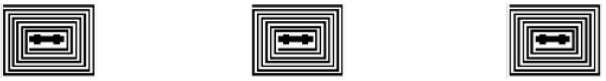

Fig. 8 Extracted watermark bit maps for frames shown in Fig. 8

Fig. 9 Extracted watermark bit maps for frames shown in Fig. 9

IV. PROPOSED WIRELESS COMMUNICATION ARCHITECTURE

As mentioned Section II and III, the CWA algorithm has been presented and the performances are demonstrated, respectively. To realize in the feasible system, we extend the CWA to the communication system to achieve the functions of post-compression and content authentication. Fig. 10 illustrates the block diagram for the proposed wireless communication architecture combined with CWA algorithm. The watermarks are first preset to insert to the video contents. As the residential viewer requests the video sever system, the assigned watermarked content is then transmitted to the CAVLC-based decoder which located in the mobile station. Thus the

watermarks are extracted to estimate the video quality. Accordingly, the billing information relying video quality can be determined and forwarded to the video stream server. Consequently, the billing fee can be determined relying the quality information by the video content sever.

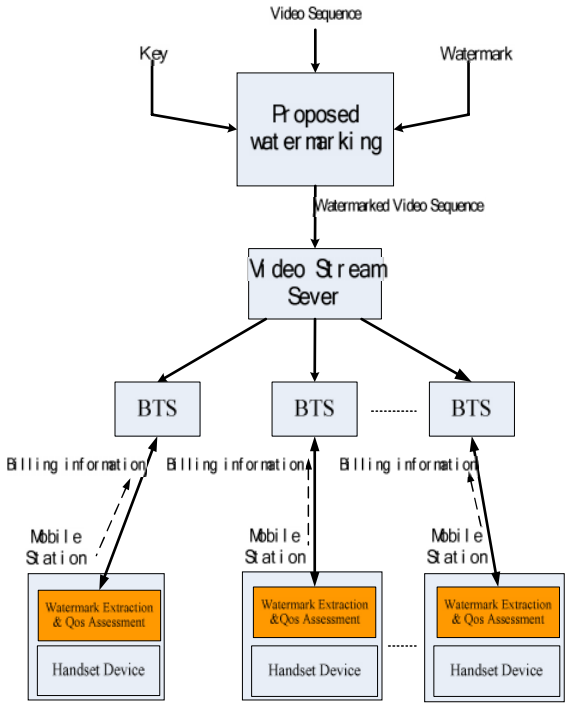

Fig. 10 Block diagram for the proposed wireless communication system

V. Conclusion

This paper has presented a novel fragile watermarking scheme for the authentication and post-compression of H.264/AVC video streams. The simulation results have shown that the proposed scheme causes an imperceptible degradation of the video quality at the receiver end and facilitates the authentication of both the I-frames and the P-frames within the transmitted video sequence. Significantly, the watermark information is embedded in the final non-zero coefficient of each quantized DCT block, and thus the watermarking scheme yields a potential reduction in the size of the watermarked file. In other words, the proposed scheme not only provides an authentication capability, but also reduces both the transmission time and the storage space requirements of the H.264 video content.

Acknowledgment

The authors would like to thank the National Science Council of the Republic of China, Taiwan for supporting this research publication. (NSC- 99-2218-E- 006-239- and NSC-99-2221-E-471-002-).

References

[1] F. Bartolini, A. Manetti, A. Piva and M. Barni, "A data hiding approach for correcting errors in H.263 video transmitted over a noisy channel," *2001 IEEE Fourth Workshop on Multimedia Signal Processing*, pp.65-70, Oct. 2001.

[2] M. Chen, Y. He, and R. L. Lagedijk, "A fragile watermark error detection scheme for wireless video communications," *IEEE Trans. Multimedia*, Vol. 7, No. 2, , pp. 201-211, Apr. 2005.

[3] P. Zhou and Y. He, **"**A fragile watermark error detection scheme for JVT," *2003. ISCAS '03. Proceedings of the 2003 International Symposium on Circuits and Systems*, vol. 2, 25-28 May, 2003, pp.956-958.

[4] C. B. Adsumilli, M. C. Q. Farias, S. K. Mitra, and M. Carli, "A robust error concealment technique using data hiding for image and video transmission over lossy channels," *IEEE Trans. Circuits Syst for Video Technol.*, vol. 15, no. 11, pp. 1394-1406, Nov. 2005.

[5] W.-N. Lie, T. C.-I. Lin, C.-W. Lin, "Enhancing video error resilience by using data-embedding techniques," *IEEE Trans. Circuits Syst. Video Technol* ., Vol. 16, No. 2, pp. 300-308, Feb. 2006.

[6] *Advanced Video Coding*, I. 14496-10 and I. R. H.264, 2003.

[7] C. C. Wang, Y. C. Hsu, "Fragile Watermarking Scheme for H.264/ Advanced Video Coding Streams," *Optical Engineering*, vol. 49, Issue2, pp.027003-027012, Feb, 2010.