International Journal of Security and Its Applications
Vol.8, No.4 (2014), pp.239-246
http://dx.doi.org/10.14257/ijsia.2014.8.4.21

Research and Implementation of an Integrity Video Watermarking Authentication Algorithm

Guochuan Shi[1], Guanyu Chen[1],Binhao Shi[2], Jiangwei Li[1] and Kai Shu[1]

[1]*Army Officer Academy.451,Huangsan Road,Hefei,Anhui,P.R.C*
[2]*Anhui Medical University.81,Meishan Road,Hefei,Anhui,P.R.C*
E-mail:1115095572@qq.com

Abstract

The integrity video watermarking authentication algorithm is proposed based on DCT coefficients. Because of the characteristic of vulnerable to interference for high-frequency DCT coefficients, we use the relationship between the average energy of the high frequency coefficients and the energy of every the high frequency coefficients and Substitution cipher to beneficiate the Image Watermarking. The result is embedded in the intermediate frequency coefficients. Experimental results show that image of minor attacks will cause severe deformation so that it is difficult to extract the identifiable watermark. It can achieve the integrity authentication purposes.

Keywords: video watermarking, integrity authentication, DCT coefficients

1. Introduction

In the information security, integrity of the information is one of the important issues [1, 2]. Integrity Certification is a technology of discovering information tampering and verifies information integrity and accuracy. According to different levels of authentication, integrity authentication includes content-level integrity authentication and data-level integrity certification. Content-level certification is certification of Content changes who is allowed some modifications on carrier, data-level certification is that any modification of the vector is sensitive. Digital watermarking is playing an increasingly important role in the aspect of identification of digital media content integrity and authenticity. This paper mainly focuses on research and practice about video watermarking combined with the standard of H.264/AVC [3, 4].

Currently video watermarking algorithm is divided into methods based on the original video and based on compressed video [5]. Watermarking algorithm based on the original video embed watermarking information into the untreated encoded video stream data and watermarking algorithm based on compressed video combines with video compression standard to embed watermarking information when encoding video or after encoding video. The video watermarking algorithm that was proposed by Kalker, *et al.*, based on radio communication monitoring theory belongs to the original video watermarking algorithm [6]. But few original video watermarking algorithms are used to video integrity certification, so this paper studies watermarking algorithm based on the compressed video to verify the video integrity. Chen, *et al.*, proposed watermarking algorithm that use AC coefficients of the modified DCT (Discrete Cosine Transformation) coefficient block to complete semi-fragile watermark embedding based on compressed domain [7]. But it will cause changes in the video bit rate and is likely to cause distortion of the cumulative. Langelaar, *et al.*, [8], who proposed a selectively discarded portion of the AC coefficients of DCT transform method to embed the

ISSN: 1738-9976 IJSIA

watermark, Watermarking information bits through the energy difference between the high-frequency coefficients of the DCT coefficients to encode, so this watermarking technique is called DEW (Differential Energy Watermarking) Differential Energy Watermarking which is considered a classic compressed video watermarking algorithm. This scheme is proposed based on the algorithm.

2. Watermarking Information Pretreatment

If the watermark information is not processed but directly embedded in the video so that the watermark information is not random, it is easily discovered by an attacker to destroy the embedded watermark.

In general, the characteristic information of the compressed video has the video quantization parameter(QP), macro-block coding pattern(CBP), Size of the relationship of DCT low frequency quantized AC coefficients, the relationship between energy of different DCT blocks, and so on [9]. H.264 uses the 4 × 4 Integer DCT transform. The frequency coefficients of the transformed are the characteristics of high energy, coefficient of stability. While the high frequency coefficients are low energy, easy interference. We use the comparison results of the watermarked coefficient block's A_{12}-A_{15} coefficients energy size and its average value to preprocess the watermark for authentication watermarking integrity.

$$E = \begin{cases} 0, & sqrt\left[\frac{1}{4}\left(\sum_{k=12}^{15} A^2(k)\right)\right] \geq A^2(k) \\ 1, & sqrt\left[\frac{1}{4}\left(\sum_{k=12}^{15} A^2(k)\right)\right] < A^2(k) \end{cases} \quad (1)$$

In this paper, the pretreatment of the watermark information is as follows: The XOR result of image watermark sequences and random sequences is encrypted with the replacement password methods, as shown in Equation:

$$M = \left\{ M \,\middle|\, M = p \oplus E', \quad 0 < E'_j < n \right\} \quad (2)$$

$$W = F(M, K_e) \oplus s = \left[\left(M_{k(1)}\right), \left(M_{k(2)}\right), \cdots, \left(M_{k(n)}\right) \right] \oplus s = (W_1, W_2, \cdots W_n) \quad (3)$$

Where p is the image watermark sequence, E′ is the deformation of E After circulating and E′ and P have the same number of bits. "⊕" is the XOR operator. F(*) indicates the encryption algorithm. "Ke" is replacement key and "s" is the random sequence. According to replacement password definition, the replace key space size is n！.Because the encrypted M-sequence reordering, it can improve the security of the watermark. For an attacker, the probability of getting the correct replacement key is 1/ n！. After the XOR, 0 and 1 in the watermark information appear in almost equal probability, and irregular distribution, similar to the noise to ensure the safety of the watermark.

3. Watermark Embedding Algorithm

In this scheme, the luminance component of the macro-block is divided into 16 4 × 4 block. Each 4 × 4 luminance component block has 16 transform coefficients after DCT transform, no matter which prediction mode is used [10]. Then arrange the coefficients according to the Zig-Zag scanning and get 16 quantized coefficients. Is quantized DC coefficient, A_1-A_{15} indicating quantized AC coefficients? We select 4 intermediate frequency coefficients A_8-A_{11} to construct a loop to embed the watermark by modifying the value of

intermediate frequency coefficients adaptively. Assume that the value of selected intermediate frequency coefficient is $Y_{i,j}$ according to the rule on the quantification:

$$Y_{q(i,j)} = quant\left[Y_{i,j}, QP\right] = round\left(\frac{Y_{(i,j)}}{Q_{step}}\right) \qquad (4)$$

where QP is the quantization parameter and Q_{step} denotes the quantization step, $Y_{q(i,j)}$ is the quantized coefficient corresponding to $Y_{(i,j)}$.

In order to improve the self- adaptability of watermark embedding, we set up local control gain factor β.

$$\beta = sqrt[\frac{1}{8}\sum_{k=6}^{14} A^2(k) - Y^2_{(i,j)}] \qquad (5)$$

$$\varepsilon = quant[\beta, QP] \qquad (6)$$

where represent the value of average energy and quantized average energy respectively.

Assuming the corresponding coordinate point (i,j) of the watermark information is W. According to the selected coefficient $Y_{q(i,j)}$, we can modify the strength of the watermark information W. The modified watermark signal is $W_{(i,j)}$. The following formula:

$$W_{(i,l)} = sign\left(Y_{q(i,j)} \cdot \alpha \cdot \beta\right) \qquad (7)$$

where α is the factor that control the embedding strength. The watermark signal quantization:

$$W_{q(i,j)} = quant\left[W_{(i,j)}, QP\right] \qquad (8)$$

The watermarking algorithm using the following formula to modify the selected quantized coefficients:

$$Y^*_{q(i,j)} = \begin{cases} \varepsilon & \text{if } \left|W_q(i,j)\right| < 1 \\ \varepsilon + W_q(i,j) & \text{if } W(m) = 1 \text{ and } \left|W_q(i,j)\right| \geq 1 \\ \varepsilon - W_q(i,j) & \text{if } W(m) = 0 \text{ and } \left|W_q(i,j)\right| \geq 1 \end{cases} \qquad (9)$$

Where W(m) is the binary watermark bits to be embedded. When implemented, according to the above judgment condition, $Y_{q(i,j)}$ is changed to $Y^*_{q(i,j)}$, then begin the entropy encoding.

4. Extraction and Integrity Judgment of the Video Watermark

In this algorithm, all I-frame video is embedding the same watermark. So if any group of I-frame in the GOP frame image is founded when extracting the watermark, watermark information can be extracted. Because the proposed scheme does not need participation of the original video when extracting the watermark, we can achieve the blind watermark extraction. Watermark extraction procedure is as follows: according to the header information of the frame and macro-block, find the divided a 4 × 4 transform block quantization coefficients of the I-frame image macro-block, and then find out the quantization coefficients $Y^*_{q(i,j)}$ corresponding to the embedded position.

Finally, do the following judgment:

$$W(m)=\begin{cases} NULL & \left|Y^{*}_{q(i,j)}\right|=\left|\varepsilon\right| \\ 1 & \left|Y^{*}_{q(i,j)}\right|>\left|\varepsilon\right| \\ 0 & \left|Y^{*}_{q(i,j)}\right|<\left|\varepsilon\right| \end{cases} \quad (10)$$

Depending on the type, extract the watermark information after pretreatment.

In the pretreatment of watermark information, we use the high-frequency energy value to pretreat watermark. In the watermark recovery, we need to calculate the high-frequency energy value when decoding. And by the equation (1) again comparing the average high-frequency energy value with each of the high-frequency energy value to get the value of E. Because the high frequency coefficients are low energy, easy interference, E value sequence may result in a change if the video is attacked and it seriously affect the recovery of the watermark information. Finally, we cannot get the correct watermark information, so as to achieve the integrity authentication of watermark.

Part of the code as follows:

```
void embed(int i,int j,int m7[][4],int wmm)
{
        int k,l;
        int e=0,p;
        int temp=0,coeff_ctr;
        int m,mq;
    for (coeff_ctr=1;coeff_ctr<12;coeff_ctr++) // set in AC coeff
        {
         // Alternate scan for field coding
         k=scan[coeff_ctr][0];
         l=scan[coeff_ctr][1];
         temp=(int)pow(m7[l][k],2);
         e+=temp;
        }
         p=(int)sqrt(0.05*e/10);
         m=(int)(m7[i][j]*p*0.0005);
         mq=abs((int)floor(m/28));
   if(wmm==0)
   m7[i][j]=0;
       else
                if((wmm==1)&&(mq>=abs(m7[i][j])))
    {
                        if(mq==0)
                                m7[i][j]=wmm;
                        else
                                m7[i][j]=sign(mq,m7[i][j]);
     }
   }
```

5. Experimental Results and Analysis

The experiment adopts H.264 coding standard reference software JM8.6. Operating environment is windows XP system. The test frames are the standard references frame “foreman”,” News”,” Silent” and ” Clair”. The structure of the test video frame is the IPP format and a total is 30 frames. QP is 28. The video size is 144 × 176. The experimental results are as follows:

(1) Subjective evaluation of video images before and after embedding the watermark

(a) before embedding (b) after embedding.

Figure 1. Subjective Evaluation of Video Images

From Figure 1, we can see that the watermark is hidden while the video quality subjectively doesn't have significant decrease.

(2)Video quality objective assessment

Table 1. The PSNR of the Test Sequence

Test Sequence	*The Value of PSNR*		
	Before Embedding	*After Embedding*	*Decrease*
Foreman	37.16	36.07	2.93%
News	37.31	36.01	3.48%
Silent	36.15	35.79	1.00%
Clair	40.64	39.16	3.6%

From the Table we can see that this scheme can guarantee the quality of video, although the watermarked video quality declined slightly.

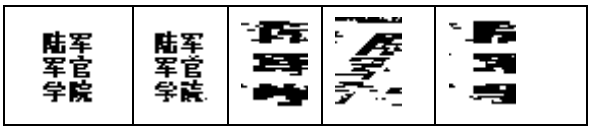
(3)Integrity verification experiment

In the experiments we evaluated the scheme against some common signal processing attacks including "salt and pepper noise", "Gaussian noise" and "circular emerging filter" and respectively extracted watermark image. As shown in Table 2.

From the above we can see that when the video sequence suffering the above attacks, the watermark image is destroyed so that the watermark image is difficult to identify. When not those attacks, the extracted watermark image can be completely identified and NC coefficient is 0.9836. This is due to the high frequency coefficients are susceptible to interference. Added noise destroys the energy relationship of high frequency coefficients and the cycle of the high frequency coefficients amplify the mistake so that the extracted watermark image is distorted serious. The algorithm implements intuitively watermark integrity certification. The disadvantage is that it cannot achieve content-level certification.

Table 2. Watermark Image Comparison

P \ *A*	*Watermark Image After The Attack*			
Original Watermark Image	*No Attack*	*Salt And Pepper Noise*	*Gaussian Noise*	*Circular Emerging Filter*



6. Conclusions

In this paper, we used the characteristics of DCT quantization high frequency coefficients to pretreat the watermark through the comparison of high frequency coefficients energy and Encrypted the watermark. Then we embed the watermark information in the frequency coefficients of 4 × 4 I-frame luminance component. Watermark extraction algorithm is simple and this algorithm achieved integrity of the video certification.

Acknowledgment

The authors would like to thank researchers at Hefei University of Technology for her excellent support. Especially we are grateful to Keke Hu at Hefei University of Technology for their valuable assistance with the experiments.

References

[1] M. Wu and B. Liu, "Data hiding in image and video: part 1—fundamental issues and solutions", IEEE Transactions on Image Processing, vol. 12, no. 6, **(2003)**, pp. 685-695.
[2] H. Xihui and F. Gui, "Digital Video Watermarking Algorithm based on H.264 Bitstream", Communications Technology, vol. 46, no. 4, **(2013)**, pp. 16-21.
[3] W. Xu and R. Wang, "H.264/AVC Video Watermarking Algorithm Against Requantization Transcoding", Journal of Electronics & Information Technology, vol. 35, no. 5, **(2013)**, pp. 1229-1235.
[4] T. Wiegand, G. J. Sullivan and G. Bjontegaard, "Overview of the H1264/ AVC Video Coding Standard", IEEE Trans on Circuits and Systems for Video Technology, vol. 13, no. 7, **(2003**), pp. 2560-2576.
[5] J. Shen and Q. Hu, "A Robust Video Watermarking Algorithm in H.264 Compressed Domain", Journal of Zhengzhou University (Engineering Science), vol. 34, no. 5, **(2013)**, pp. 63-67.
[6] T. Kalker, G. Depovere and J. Haitsma, "A video watermarking system for broadcast monitoring", Proceeding of SPIE on Security and Watermarking of Multimedia Contents, vol. 1, no. 1, **(1999)**, pp. 103-112.
[7] H. Chen, Z. Y. Chen and X. Zeng, "A novel reversible semi-fragile watermarking algorithm of MPEG-4 video for content authentication", Proceedings of the Second International Symposium on Intelligent Information Technology Application, vol. 3, no. 3, **(2008)**, pp. 37-41.
[8] C. Gerrit, R. L. Langelaar and Lagendijk, "Real-time Labeling of MPEG-2 Compressed Video", Journal of Visual Communication and Image Representation, vol. 9, no. 4, **(1998)**, pp. 256-270.
[9] M. Wang, Q. Pei and K. Fan, " H.264 video integrity authentication scheme based on fragile watermarking", Journal of xidian university, vol. 34, no. 5, **(2007)**, pp. 823-825.
[10] X. Ling and B. Gao, "A Compressed Domain Video Watermark Algorithm for Copyright Protection", Computer Engineering, vol. 39, no. 6, **(2013)**, pp. 194-199.

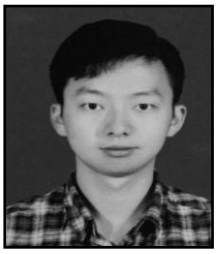
Authors

Guochuan Shi, full Professor in Faculty of omputing Center, Army Officer Academy, Hefei, Anhui, P. R. C. Computer Network and Information Security, Email: 1115095572@qq.com

Guanyu Chen, Master Graduate Student of Computing Center, Army Officer Academy, Hefei, Anhui, P.R.C. Software Engineering, Email: 289445542@qq.com

Binhao Shi, Master Graduate Student in The First Clinical College, Anhui Medical University, Hefei, Anhui, P. R. C. Clinical Medicine,Email:,847886879 @qq.com

Jiangwei Li, Master Graduate Student in Computing Center , Army Officer Academy, Hefei,Anhui,P.R.C. Computer Application, Email: 289445542 qq.com



Kai Shu, Faculty of Computing Center, Army Officer Academy, Hefei, Anhui, P.R.C. Computer Network and Information Security, Email: 307121489@qq.com