A Video Watermark Achievement Algorithm Based on Content of the Video Sub-Region

Huimin Zhao
Guangdong Polytechnic Normal University, Guangzhou, 510665, China
Email: zhaohuimin@tom.com

Dong Zhang
Sun Yat-Sen University, Guangzhou, 510006, China
Email: zhangd@mail.sysu.edu.cn

***Abstract*— Resisting collusion attack is one of important performances of video watermark algorithm. This paper presents a novel video watermark algorithm based on the visual features of the host video. The proposed algorithm embeds watermark on the DWT coefficients of sub-regions. The mechanism of JND (just-noticeable distortion) is used to attenuate the embedding strength in the sub-region. Experimental results show the proposed scheme can effectively resist two types of linear collusion attacks while still being robust, stable and imperceptible.**

***Index Terms*—video watermark, collusion attack, content, sub-region**

I. INTRODUCTION

Recent years have witnessed the great trend to distribute and share digital multimedia on the Internet. At the same time, some sophisticated software makes it feasible to manipulate digital data even by people without professional training [1]. To protect the intelligence property of the multimedia products and promote the related services, ensuring the suitable distribution and usage of multimedia content has become a more critical issue than ever before. The video watermark is capable of providing multimedia data with the desired protection during transmission, which disappears after the data are decoded into clear text [2, 3]. The big challenge the video watermarking technique confronting with is to resist collusion attack which means several users (colluders) combine several copies of the same video content embedded with different fingerprints and try to remove or attenuate the original watermark or fingerprints [1]. Developing video watermarking technology with high performance to resist collusion attack has become one of the focuses in the research domain of information security communication [4, 5, 6]. Although a lot of video watermark algorithms have been presented in the past years, the problem to improve the efficiency of resisting linear collusion attacks in real applications, especially for information security commu-nication system, is still open. Boneh et al availably resist collusion attack [7]. However, the required amount of distribution of fingerprinted copies limited to the application of this algorithm. Vinod and Bora put forward a video watermark algorithm in wavelet domain, which can resist partially collusion attacks [8]. Funda et al analyzed the features of the video watermark and resisting collusion attack in detail, and proposed a method of resisting collusion attacks by controlling the amount of the watermark distribution [9]. Because the method controls the watermark amount, the collusion attackers gained very few of the watermark information in [9]. Su and Kundur presented a vision invisibility theory, and designed a video watermark method based the video content for resisting linear collusion attacks [10].

A joint fingerprint and decryption scheme was proposed in [11]. In their work, the content owner encrypted the extracted features from the host signal with a secret key K_S, which is known to the content owner only, and multicasted the encrypted content to all users, and then transmitted to each user i a unique decryption key $K_i \neq K_S$. At the receiver's side, each user partially decrypted the received bit stream, and reconstructed a unique version of the original host signal due to the uniqueness of the decryption key. In [11], the fingerprint information is essentially the asymmetric key pair (K_S, K_i), and the unique signature from the partial decryption is used to identify the attacker or colluders.

Most previous work considered applications where the goal of the fingerprinting system is to resist collusion attack by a few colluders, and designed the efficient distribution schemes according to [11-13]. In this paper, we combine essentiality of the video content with digital watermarking and propose a novel video watermark algorithm for resisting collusion attacks.

The paper is organized as follows. We begin in Section II with the analysis requirements of selecting of the watermark embedded sub-region in video image applications, then show achieving process of the watermark embedding and extracting by computing JND value. Section III describes the experiment results in

Manuscript received January 1, 2013; revised June 8, 2013; accepted July 5, 2013.
HuiMin Zhao is with the Guangdong Polytechnic Normal University, China.
Dong Zhang is with the Sun Yat-sen University, China.

doi:10.4304/jsw.8.11.2962-2966

detail based on the proposed algorithm, and analyses the results. Conclusions are drawn in Section V.

II. THE WATERMARK ALGORITHM BASED ON CONTENT OF THE VIDEO SUB-REGION

There are two scenarios of collusion attack for the video watermarking systems. One is the attacker accesses different video copies embedded with same watermark data, and the other is the attacker has video copies have same content but different embedded watermarking. The purpose of the attacker is to remove or attenuate the original watermarking by utilizing a large mount of redundancy information between different frames. Considering characteristics of the collusion attack with visual characteristic of the video frames, here we present a novel watermark algorithm of combining embedded location with the video content.

A. Selection of Watermark Embedding Region

Considering a $d \times d$ region within a sub-band of DWT coefficients, we denote the center of this region as (m,n). Then the set $C_d(m,n)$ of the sub-bands coefficients is described as follows:

$$C_d(m,n)=\{(m+\delta_m,n+\delta_n),\quad \delta_m,\delta_n \in \{-\left\lfloor \frac{d}{2} \right\rfloor,\cdots,\left\lceil \frac{d}{2} \right\rceil -1\}\} \tag{1}$$

There are two constrains a watermarking algorithm subjects to. One is the stability which means the attacking should not change the location of watermarking. The authorized user will be able to locate where is the watermarks embedded in even after the attacking performed. The other constrain is the imperceptibility which means the embedding of watermark will not arouse perceptible distortion.

Therefore, considering above two constrains, the paper proposes a region selecting algorithm of the subbands coefficients in the video frame. The algorithm cooperates with method of extracting features of the images in the computer vision field, and estimates whether some regions are suitable to be embedded with the watermarks, according to the relationship between the subbands coefficients of low frequency and high frequency as well as middle frequency in DWT domain. The algorithm is described in detail as follows.

● Assume that *X(m,n)* is a spatial location of a subband coefficients after using DWT. The largest local noise of *X(m,n)* is defined as follow:

$$M(m,n)=\max_{|i-m|,|j-n|\le 1} |X(i,j)-X(m,n)| \tag{2}$$

The largest local noise demonstrates a boundary value of local distortion within a region which is center at (m,n). The boundary value is dependent with features of the image, and independent with location of the subband coefficients. As a result of experiment, the region with the largest local noise absorbs more energy of the watermark. Thus embedding the watermark in this region can resist more intensity attack.

●Average value of the largest local noise, $\bar{M}_d(m,n)$, is calculated in a region of $d \times d$ as follow:

$$\bar{M}_d(m,n)=\frac{1}{d^2}\sum_{(m^d,n^d)\in N_d(0,0)} M(m+m^d,n+n^d) \tag{3}$$

●Intensity value of every region, *S(m,n),* is calculated as follow:

$$S(m,n)=\min_{(m',n')\in N_3(m,n)} |\bar{M}'_d(m',n')-\bar{M}_d(m,n)| \tag{4}$$

Here, $N_3(m,n)$ denotes a 3×3 neighboring region of the coefficient *X*(*m*,*n*). $\bar{M}'_d(m',n')$ is the average value of the largest local noise of a region within the corresponding subband of watermarked video frame. (m',n') denotes the center location of this region.

●Arrange the values of *S(m,n)* within the concerned subband in a descendent order, and choose a set of the center point of non-overlapping regions by utilizing greedy algorithm.

●The subband coefficients of the DWT is divided into four parts: the approximate part *LL*, the horizontal direction part *HL*, the vertical direction part *LH*, and the diagonal direction part *HH*. We denote the *LH*, the *HL*, and the *HH* by symbol *L* , *M* , and *H*, respectively. Then, those symbols respectively express the sum of absolute value of DWT coefficients in the sub-region. Therefore, we can evaluate regions which is suitable for embedding watermark according to the relationship among *L*, *M* , and *H* [16]. The relationship of absolute of these values is determined according to practical experiment as shown in the section of III.

As a natural scene of a video frame usually show more energy in its lower frequency domain, and less higher frequency energy, the values of *M* and *H* are small, and the value of *L* is larger. Based on the experiment result and the content of video, we found selecting the regions with smooth contents will benefit the watermarking performance of resisting collusion attack. That is to say, those regions can absorb more energy of the watermark. Therefore, the algorithm shows better stability and robustness.

B. Computing JND value based on the HVS

The JND (just-noticeable distortion) is a value of the largest distortion of HVS (human visual system), and is a visual model applied for video watermarking research. In the paper, value of the JND needs to be estimated in DWT zone. Different from general methods of computing JND, this paper will give an effectual calculation method.

First, a function of difference sensitivity is calculated. Assume that $g(i,j,n)$ is the function, and denotes a value of the function of difference sensitivity in location (i,j) of the *n*th DWT subband. Then, the $g(i,j,n)$ is calculated as follow.

$$g(i,j,n)=c_0\left(k_1+k_2\left|\ln\left(\frac{\varepsilon\upsilon}{3}\right)\right|^3\right)\upsilon(2\pi\rho_{ij})^2\cdot\exp\left(-2\pi\rho_{ij}c_1\frac{(\varepsilon\upsilon+2)}{k_3}\right) \tag{5}$$

Here, the values of $c_0, k_1, k_2, k_3, \varepsilon, \upsilon$ are constant, respectively. *i, j*=0,1,…,*d*. ρ_{ij} is the spatial subband frequency at the *d*×*d* sub-region, and the value of the ρ_{ij} is computed as follow.

$$\rho_{ij} = \frac{1}{2N}\sqrt{\left(\frac{i}{\omega_x}\right)^2 + \left(\frac{j}{\omega_y}\right)^2} \tag{6}$$

Where $\omega_x and\ \omega_y$ denote an angle between the horizontal and vertical direction of the subband location (*i*,*j*).

Secondly, assume that $a_{Lum}(n)$ is an adjusted luminance coefficient on *n*-level decomposition of DWT, then the $a_{Lum}(n)$ is computed in the *d*×*d* sub-region. The $a_{Lum}(n)$ shows average luminance in the sub-region, and has a relation with *LL* coefficient as formula (7).

$$a_{Lum}(n) = \begin{cases} 2\times\left(1-\dfrac{LL(n)}{4M}\right)^3 + 1, & LL(n) \le 4M \\ 0.8\times\left(\dfrac{LL(n)}{4M}-1\right)^2 + 1, & otherwise \end{cases} \tag{7}$$

Here, *M* denotes gray level of the frame, and value of the *M* is 256 generally.

Therefore, overall JND value is computed as follow.

$$JND(i,j,n) = A\frac{a_{Lum}(n)}{g(i,j,n)}\frac{M}{\varphi_i\varphi_j(L_{\max}-L_{\min})} \tag{8}$$

where $L_{\max} and\ L_{\min}$ are the maximum and the minimum values of the gray in present frame, respectively. φ_i and φ_j are respectively factors of standardization DWT. *A* is an experience constant obtained by a large number of experiments.

C. Process of the Watermark Embedding and Extracting

In [17], Malvar et al proposed an improved spread spectrum watermarking scheme (ISS) . By adapting to the host, as the source of interference, ISS achieves significant improvement in terms of robustness performance. According to the principle of embedding watermark of the spread spectrum technology, we assume that $X(i,j,n)$ is the original video frame extracted from video sequences, $W(i,j,n)$ is the watermarking information; $Y(i,j,n)$ is the watermarked video frame. Then, the watermark embedding function is given as follows:

$$Y(i,j,n) = X(i,j,n) + JND(i,j,n)W(i,j,n) \tag{9}$$

When the watermarks are embedded, the value of JND(*i*,*j*,*n*) is regarded as modulation coefficient of the spread spectrum.

When the watermarks are extracted, the algorithm firstly estimates the original video frame. For the video frames $Y(i,j,n)$ of the embedded watermarks, we use median filter or mean filter of 3×3 neighborhood to obtain the estimated $\overline{X}$ of the *X*, and to obtain the estimated value $\overline{JND}$ of the *JND*. Finally, we can estimate the values of the watermarks as follows in formula (10).

Therefore, we can decide whether or not the video frames contain the watermarks by using correlation detection

$$\overline{W}(i,j,n) = \frac{Y(i,j,n) - \overline{X}(i,j,n)}{\overline{JND}(i,j,n)} \tag{10}$$

between the extracting watermarks and the original watermarks. A normalized correlation coefficient is defined as:

$$\sigma(W,\overline{W}) = \frac{\sum_{i=1}^{N} w_i \overline{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2 \sum_{i} \overline{w}_i^2}} \tag{11}$$

Where, $W = \{w_i, i = 1,2,...,N\}, \overline{W} = \{\overline{w}_i, i = 1,2,...,N\}$, *N* is the length of the watermarks, respectively. If the correlation coefficient $\sigma(W,\overline{W})$ is greater than the pre-specified threshold *T*, then the watermark has been detected.

III. Experiment Results and Discussions

As mentioned in section II, both locations and process of the embedded watermark depend on the visual characteristics of the video image. Therefore, the algorithm possesses a better robustness to resist the collusion attacks. Simultaneously, the algorithm uses the JND to control the strength of the embedded watermarks based on the spread spectrum technology, so it also possesses a better performance to resist general attacks of signal processing. In this paper, the value of *PSNR* is controlled at between 36-39dB after embedding the watermarks, and the collusion attack and the general attack of signal processing and compressed attack are tested by using the akiyo.yuv and mobile.yuv video sequences of 352 × 288 CIF format [16]. The original video images are decomposed into four level using Haar Wavelet. In practical experiment of the paper, we select *M*+*H*>151 and $\frac{L}{M} \ge 2.8 or \frac{L+M}{H} \ge 1.6$, and $\frac{L}{M} \ge 1.8 or \frac{L+M}{H} \ge 40$ as the sub-region of embedding the watermarks.

A. Test for the First Scenario of the Collusion Attacks

Assume that $Y_1, \cdots, Y_N$ are various video frames possessed variable pictures, these frames are embedded with the same watermark *W* based key controlling. The watermarks $\overline{W}_1, \cdots, \overline{W}_N$ are estimated from the $Y_1, \cdots, Y_N$, respectively. After averaging $\overline{W}_1, \cdots, \overline{W}_N$, we obtained

the value of the estimated watermark $\overline{W}$. In addition, the video frame Y is subject to attack. After being attacked, we can obtain the frame $\overline{Y}$ from Y by removing $\overline{W}$. Finally, the watermarks is extracted directly from $\overline{Y}$. In the test scheme, we use a mixed video of the length of forty-six frames. In the experiment, for every frame, we utilize other forty-five frames to estimate the Gauss sequence watermarks. The experiment results are shown in Fig.1.

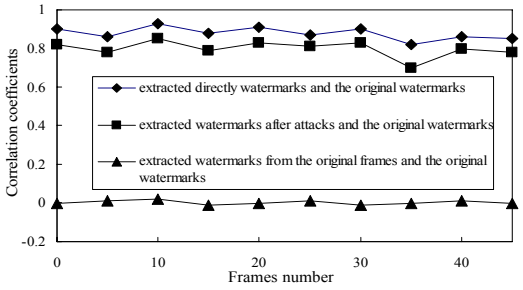

Fig 1. Experiment results of the test scheme I

B. Test to the Second Scenario of the Collusion Attacks

Assume that $Y_1,\cdots,Y_N$ are some successive video frames which have similar contents. Distinct watermarks $W_1,\cdots,W_N$ are embedded to every frame of the video frames. After averaging $Y_1,\cdots, Y_N$, we obtain the values of the attacked $\overline{Y}$. We may extract directly the watermarks $\overline{W}$ from $\overline{Y}$, and detect the correlation of the $\overline{W}$ and the $W_1,\cdots,W_N$. Finally, we can decide the video frames whether or not included the Gaussian sequence watermark by the correlation coefficient. The experiment results are shown in Fig.2.

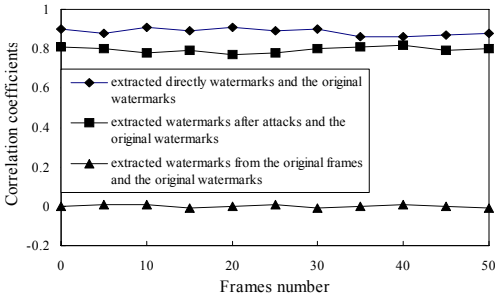

Fig 2. Experiment results of the test scheme II

From the above experiment results, we find that at the same location the extracted correlation coefficients before the embedding is clearly different from the ones obtained from the embedded video frame. This shows that the watermarks information has been indeed embedded into the video streams, and proves the existence performances of the watermark. On the other hand, compared with the correlation coefficients extracted from the embedded video frame, the one obtained from the attacked embedded video frame has almost the same value. This also shows the watermark possesses better robustness for the collusion attack.

C. Test of Adding Random Noise

In the test, the experiment environment is same with case *A* besides the embedded watermarks. We add the random Gauss noise to every frame in frequency domain, and calculate the correlation coefficient after extracting the watermarks, and evaluate whether the watermark is effective. The experiment results are shown in Fig.3. The result shows that the correlation coefficient after attacked is close to the one of the original watermarks, and indicate the algorithm can resist efficiently the adding noise attack in this paper.

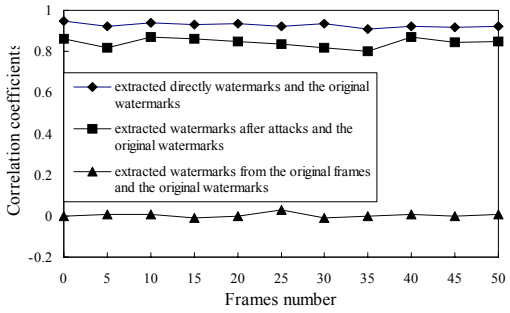

Fig 3. Experiment results of the test scheme III

D. Test of Compressed Attack

In the experiment, the video embedded the watermarks is coded and decoded according to MPEG-2 standard, respectively. Afterwards, we extract the watermarks from frontal forty-five frames, and compute the correlation coefficient, and detect the watermarks whether having loss due to compression. The experiment results are shown as Fig.4. The data of the experiment show the watermark performance against compression is dependent to location and strength of the embedded watermark. On the whole, the embedded watermark can resist partly the compressed attack. This case relates to rate controlling and GOP.

There is a need to explain this case. The algorithm can resist efficiently non-liner collusion attack because the embedding process does not operate in time domain.

The experimental results show our watermarking scheme is robust to the collusion attack. Simultaneously, the results also show the feature selection region of the algorithm is stable. The results also confirm that the algorithm achieves the purpose of resisting the collusion attack because the content based video watermark scrambles the location of embedding. In addition, the algorithm improves the imperceptibility of the video watermarks because the algorithm uses the JND value to modulate the spread coefficients.

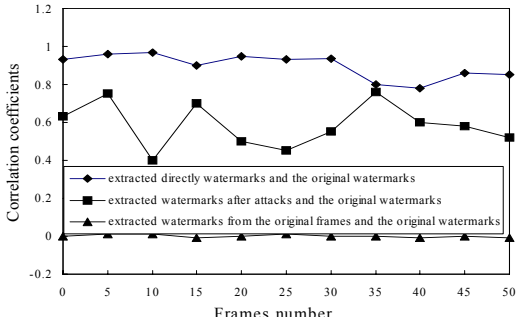

Fig 4. Experiment results of the test scheme V

V. CONCLUSION

Based on features region selecting of the video content, the paper proposes a novel video watermarks algorithm for resisting the collusion attack. According to the visual characteristics of the image and the relationship between DWT subbands coefficients, the region of watermarks embedding may be randomly selected. Because of the consideration of the visual characteristics, these regions have a better stability, and can contain more watermarks energy. Simultaneously, there is no fixed pattern for the sub-regions of embedding, and the algorithm can efficiently resist the general signal processing attack. The experiment results demonstrate the effectiveness of this algorithm.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (no.61272381), Natural Science Foundation of Guangdong of China (no.S2012010008639), and Guangdong Province Science and Technology Plan Project (no.2012B010100035).

REFERENCES

[1] H. Vicky Zhao, and K. J. Ray Liu. 'Fingerprint Multicast in Secure Video Streaming", IEEE Transactions on Image Processing, vol. 15, no. 1, pp.12-29, January 2006.

[2] K.Gopall, M.Madhavi Latha. 'Watermarking of Digital Video Stream for Source Authentication", IJCSI International Journal of Computer Science Issues, vol.7, no. 1,pp.18-25, July 2010.

[3] W.M.Chen, C.J.Lai, H.C.Wang, et al. 'H.264 Video Watermarking with Secret Image Sharing", IEEE Image Processing, vol.5,no.4,pp. 349-354, may 2011.

[4] Ajay Goel, O.P.Sahu. 'Improved Digital Watermarking Techniques and Data Embedding In Multimedia", (IJCSE) International Journal on Computer Science and Engineering, vol.2, no.2,pp.164-168, February 2010.

[5] Yuting Su, Junyu Xu, Bo Dong, Jing Zhang, et al. 'A Novel Source MPEG-2 Video identification algorithm", International Journal of Pattern Recognition and Artificial Intelligence, vol.24, no.8, pp.1311-1328, December 2010.

[6] S.H.Liu, L.Han, H.X.Yao. 'Video watermarking algorithm for resisting collusion attacks", Journal on Communications, vol.31, no.1, pp.14-19, January 2010.

[7] D.Boneh, J.Shaw. 'Collusion-secure fingerprinting for digital data", IEEE Trans Inform Theory,vol.44, no.5, pp.1897-1905, may 1998.

[8] P.Vinod, P.K.Bora. 'Motion-compensated inter-frame collusion attack on video watermarking and a countermeasure", IEE Proceedings Information Security, vol.153, no.2, pp. 61-73, February 2006.

[9] F.Ergun, J.Kilian, R.Kumar. A note on the limits of collusion resistant watermarks, Advances in Cryptology Eurocrypt 1999 Prague, Czech Republic.1999,pp.140-149.

[10] K.Su, D.Kundur, D.Hatzinakos. 'Statistical invisibility for collusion-resistant digital video watermarking", IEEE Transactions on Multimedia, vol.7, no.1, pp.43-51, January 2005.

[11] D.Kundur, and K.Karthik. 'Video fingerprinting and encryption principles for digital rights management", Proc. IEEE, vol. 92, no. 6, pp.918–932, Jun 2004.

[12] L.Shen, C.H.Jiang, S.G.Guo. A H.264 Video Watermarking Algorithm based on DCT Domain and MV,2011IEEE International Conference on Information Theory and Information Security, vol.1,pp. 573-576, November 2011.

[13] J.W.Lee, T.W.Oh, M.J.Lee, H.Y.Lee, et al. Video Watermarking on Overlay Layer, 2011 seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP) , 2011 IEEE Press,pp. 85-88.

[14] Anuradha, R.P. Singh. 'DWT Based Watermarking Algorithm using Haar Wavelet", International Journal of Electronics and Computer Science Engineering, vol.1,no.1, January 2012.

[15] L.Tzu-Chao, L.Chao-Ming. 'Wavelet-based copyright-protection scheme for digital images based on local features", Journal of Information Sciences, Vol.179, no.19,pp. 3349-3358, Sep 2009.

[16] Z. Dazhi, W.Boying, S. Jiebao, H.Heyan. A New Robust Watermarking Algorithm Based on DWT, 2nd International Congress on Image and Signal Processing, pp.1-6, Oct 2009.

[17] H. S.Malvar and A. F. Florencio, 'Improved spread spectrum: A new modulation technique for robust watermarking," IEEE Trans. Signal Process., vol. 51, no. 4, pp. 898–905, Apr. 2003.

HuiMin Zhao, was born in Shanxi, China, in 1966. He received the B.Sc. and the M.Sc. degree in signal processing in 1992 and 1997 from Northwestern Polytechnical University, Xian, China, respectively. He received the Ph.D. degree in electrical engineering from the Sun Yat-sen University in 2001. At present, he is a professor of the Guangdong Polytechnic Normal University. His research interests include image, video and information security Technology.
E-mail: zhaohuimin@tom.com

Dong Zhang, was born in Gansu, China, in 1974. He received the B.Sc. and the M.Sc. degree in image processing in 1999 and 2003 from school of electronics science and engineering, Nanjing University, Jiangsu, China, respectively. He received the Ph.D. degree in electrical engineering from the Sun Yat-sen University in 2009. At present, he is a instructor of the Sun Yat-sen University. His research interests include image, video and information security Technology.
E-mail: zhangd@mail.sysu.edu.cn