Authentication of Lossy Compressed Video Data by Semi-Fragile Watermarking

Tsong-Yi Chen, Chien-Hua Huang, Thou-Ho Chen, and *Cheng-Chieh Liu

chentso@cc.kuas.edu.tw, a091315107@cc.kuas.edu.tw, and thouho@cc.kuas.edu.tw
Department of Electronic Engineering, National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan 807, R.O.C., *Huper Laboratories Co., LTD

Abstract

This paper proposes an effective technique to detect and locate alterations of the tampered frame, whether it is stored again into original bit-streams or not. A block-classification strategy is used to classify DCT -blocks into the flat-block and the normal-block. Simple features of the both blocks are embedded invisibly. The damaging problem of clipping errors caused by normailization in spatial domain can be reduced significantly more than other techniques. Experimental results show that the proposed technique can detect various tampered areas and hence provide an effective image authentication for lossy compressed videos (e.g. H.263), especially for DVR (digital video recorder) security systems.

Keywords: watermarking, image authentication, compressed video.

1. INTRODUCTION

More and more applications for tamper detection include authentication of digital data for courtroom evidence and copyright protection. The reason is that the authenticated image or video will likely be maliciously tampered when they spread over internet or data-base. In the past, several techniques and concepts, such as fragile watermarks, semi-fragile watermarks, and self-embedding, based on data hiding or stenography have been introduced for tamper detection in digital images and for image authentication. One class of authentication watermarks is formed by semi-fragile watermarks. Such watermarks are marginally robust and are less sensitive to pixel modifications. Thus, it is possible to use them for quantifying the tampering degree and distinguishing simple LSB shuffling from malicious changes, such as feature adding and removal.

In [1], they propose an image tamper detection and recovery system based on the discrete wavelet transformation (DWT) technique. The research of [2] present a new authentication scheme by embedding a visually meaningful watermark and a set of simple features in the frequency domain transformed from an image via table look-up. For copyright protection of compressed video, [3] develops a watermarking technique which is appropriate for MPEG2 video coding system by extending the direct sequence spread spectrum. It also shows that various methods of the watermark embedding and extraction for video coding system. With embedding the watermark into coefficients after DCT and quantization processings, the optimal trade-off between the quality of video and robustness of authentication can be obtained. However, the clipping-error owing to normalization in spatial domain is still an intractable problem. In this paper, we propose an effective technique which can detect malicious manipulations on lossy compressed video data (e.g. H.263) and reduce the clipping-error problem. The basic idea behind the proposed method is firstly to classify DCT-blocks into the flat-block and the normal-block. To detect and locate alterations of the tampered frame, simple features are embedded into the above classified blocks invisibly. Based on pre-processing DCT coefficients before quantization, the clipping error problem resulted form normalization can be reduced significantly. For later authentication, the watermarked frame is then put back into the compressed bit streams.

2. PROPOSED WATERMARKING METHOD

The proposed watermarking process is based on 8x8-block DCT transform. The watermarking is performed on the Y component (luminance) of YCbCr color model. The basic process can be briefly described in the following.

At first, we hide the watermark into the chosen non-zero quantized AC coefficient, denoted as $NQAC_i$, by backward zigzag-scan in each block. We set a threshold τ to divide the input frame into normal-blocks and flat-blocks. If the number of those coefficients of the block is more than τ, the block is named a normal-block or otherwise called a flat-block. The following subsections will illustrate how the watermark is embedded into these two blocks.

2.1. Normal-Block Embedding

For brevity, the normal-block embedding is described in the following points.

(1)**Get a block classification bit :** A feature bit "1" is

embedded as an authentication-key.

(2)**Obtain the watermark :** We extract the watermark from the quantized DC coefficient. To emphasize the security of embedded watermark, a fast one-dimensional pseudorandom number generating approach is used to shuffle the watermark bits w_i to disperse their energy relationship via exclusive-or operation. Here, the *i* denotes *authentication strength.* Although the degree of authentication can be defined by *authentication strength*, it will make more degrade of image quality with more authentication bits, and vice versa. This is a trade-off between the quality of video and robustness of tamper detection.

(3)**Embed the watermark :** We embed the watermark bit, w_i into the LSB bit of chosen $NQAC_i$ in each block. The $NQAC_i$ will be altered by the normal-block embedding as Eq. (1):

$$NQAC_i^{'} = \begin{cases} sign(NQAC_i) * NQAC_i, \\ if\ Bit_0(|\ NQAC_i\ |) = w_i \\ sign(NQAC_i) * AF(NQAC_i), \\ if\ Bit_o(|\ NQAC_i\ |) \neq w_i \end{cases} \quad (1)$$

Where "+1" or "-1" will be selected according to the sign of $NQAC_i$. An *adjustment function*, *AF*, has two major features. In the first feature, the $NQAC_i$ "1" will be altered into "0" while w_i is "0". This will generate a data extracting fault due to the absence of the NQAC. The second feature is to transform the $NQAC_i$ "2" or "–2" into "1" or "–1". The *adjustment function* is as Eq. (2):

$$AF(NQAC_i) \Rightarrow \begin{cases} Bit_1(|\ NQAC_i\ |) = w_i \oplus 1, \\ if\ |\ NQAC_i\ | = 1 \\ Bit_1(|\ NQAC_i\ |) = w_i \oplus 1, \\ if\ |\ NQAC_i\ | = 2 \\ Bit_0(|\ NQAC_i\ |) = w_i \end{cases} \quad (2)$$

For example, according to the result of normal-block embedding, the $NQAC_i$ "1" is "1", "-2" is "-1", "3" is "3", "-4" is "-5" while w_i is "1". Other $NQAC_i$ "1" is "2", "-2" is "-2", "3" is "2", "4" is "4" while w_i is "0".

2.2. Reduction of Clipping Errors

The quantized AC coefficient will likely be corrupted while enforcing normalization in spatial domain. The clipping error may be occurred due to that all pixels must be normalized to [0,255] in spatial domain. This is a *false alarm* for tamper detection.

We can reduce the problem by two steps. The first step, we transform (DCT and quantization) again to make the fixed clipping error. The second step, we will find out maximum clipping error, and calculate its basis image from Eq. (3). The basis image with a scaling factor as a weight-mask (see Eq. (4)). Using the sign of the weight-mask to map the chosen quantized AC coefficient. Then, the maximum clipping error will not be raised any more. For example, as the Figure 1(a)(b) shown, the pixel of coordinates (1,7) is 253 that into the maximum clipping error (269) will occur, and it will affect the chosen quantized AC coefficient. The basis image *B(x,y;u,v)* is as

$$B(x,y;u,v) = \cos\frac{(2x+1)u\pi}{2N}\cos\frac{(2y+1)v\pi}{2N} \quad (3)$$

From IDCT (inverse discrete cosine transform):

$$f(x,y) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cos\frac{(2x+1)u\pi}{2N}\cos\frac{(2y+1)v\pi}{2N}$$

The basis image with a scaling factor $\alpha(u)\alpha(v)$ is as

$$\alpha(u)\alpha(v)B(x,y;u,v) \quad (4)$$

184	161	161	173	170	183	226	252
126	122	133	193	235	244	253	253
45	80	116	194	244	244	253	250
55	56	103	200	244	232	237	247
72	49	111	193	225	239	248	252
85	75	140	177	192	241	250	234
88	69	104	123	131	164	163	136
66	75	94	86	68	80	90	74

182	160	160	171	168	182	225	254
126	121	132	193	235	243	264	269
44	80	116	193	243	244	256	249
54	54	101	199	243	230	235	246
71	47	109	191	224	237	246	257
84	75	140	176	191	241	250	233
87	68	103	123	131	163	162	136
64	74	93	84	66	79	89	72

Figure 1. (a) 8x8 pixel-block (normalization); (b) 8x8 pixel-block (no normalization).

0.13	-0.17	0.16	-0.15	0.12	-0.1	0.07	-0.03
0.15	-0.2	0.19	-0.17	0.15	-0.12	0.08	-0.04
0.07	-0.09	0.09	-0.08	0.07	-0.05	0.04	-0.02
-0.03	0.05	-0.05	0.04	-0.03	0.03	-0.02	0.01
-0.12	0.17	-0.16	0.15	-0.12	0.1	-0.07	0.03
-0.17	0.24	-0.23	0.2	-0.17	0.14	-0.09	0.05
-0.16	0.23	-0.21	0.19	-0.16	0.13	-0.09	0.05
-0.1	0.14	-0.13	0.12	-0.1	0.08	-0.05	0.03

160	-28	-5	1	2	2	0	0
17	-5	1	0	2	-1	-1	0
-8	13	6	-1	-2	0	0	0
7	0	3	0	0	1	1	0
-4	3	1	-1	1	0	0	0
-1	1	0	0	0	0	0	0
0	0	0	-1	-1	0	0	0
-1	0	0	0	0	0	0	0

Figure 2. (a) weight-mask block of pixel (1,7); (b) 8x8 DCT-block *(authentication strength* is 5).

Eq. (4) is a weight-mask which can map the 8x8 coefficient from DCT domain to spatial domain. As the Figure 2(a)(b) shown, we must alter the sign of the chosen embedded 5 coefficient by weight-mask so that the pixel (269) will not be raised any more. It is useful for revertible capability of the chosen quantized coefficient.

Consequently, we can pre-process above two steps so that the chosen quantized AC coefficient can map back for the normal-block embedding.

2.3. Flat-Block Embedding

For brevity, the flat-block embedding is described in the following points.

(1)**Get a block classification bit :** A feature bit "0" is embedded as an authentication-key.

(2)**Obtain and embed the watermark :** Based on the characteristic of the few embedding capability in smooth region, we pick out the Bit_5, Bit_6, and Bit_7 as the watermark bit from quantized DC coefficient, and embed they into the authentication-key. For the better trade-off between the robust of authentication and the capacity of authentication-key, we can replace previous pseudo-random number to with Bit_0 and Bit_1 so that we have 5 watermark bits to authenticate tampering blocks. It's very useful for decreasing strength of the authentication-key and maintaining quality of the frame.

3. PROPOSED TAMPER DETECTION SCHEME

We propose the tamper detection approach as follows:

(1)**Ahead detect the tampering block :** We can use a block-classification bit to authenticate fastly the tampering block.

(2)**Tamper detection algorithm :** First of all, we extract the compared bits of the pre-selected quantized DC coefficient. Second, we recover the watermark bits from the embedded coefficient and authentication-key. Third, We can calculate the *Hamming Distance* between the watermark bit and the compared bit in each block. If the result of comparison has no difference, this block of the frame is not tampered. Otherwise, this block of frame is tampered, and the difference will be the positions of the tampered area of the original frame. We can see the proposed watermarking and tamper detection scheme as the Figure 3 shown. Where NAC denotes the number of the non-zero quantized AC coefficient in each block, the value of τ is defined according to various experimental results. The watermarked frame by using our proposed embedding approach still maintains high quality of image, and it will not raise too more bit-streams. We can see the result of the tamper detection, as shown from Figure 4 to Figure 7.

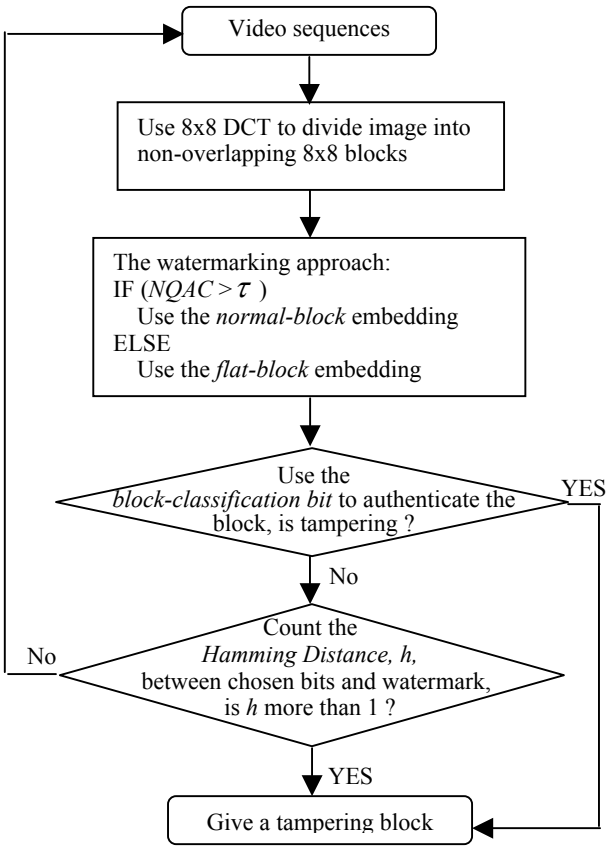

Figure 3. The proposed block-based video tamper detection algorithm.

Figure 4. original authentication frame.
(using H.263, Qp=7, bit-streams = 12169 Bytes).

Figure 5. watermarked frame.
(PSNR = 42.5 db, bit-streams = 12378 Bytes).

Figure 6. illegal tampered frame.

Figure 7. tampered area using proposed approach.

4. CONCLUSIONS

In this paper, we propose an effective technique which can detect malicious manipulations on lossy compressed video data (e.g. H.263) and reduce the clipping-error problem. Although the quantized coefficients are more suitable than original coefficients for data embedding. It is noteworthy that the damaging problem of clipping errors can be caused by normalization in spatial domain. In this paper, we can reduce the problem of clipping errors.

Besides, we cannot embed too much data into the flat (smooth) block due to the value and number of the non-zero quantized AC coefficient is small and less. So, we use a specific approach to embed the watermark into the flat-block. Further, we can try to recover the tampered frame according to the few authentication-key.

5. REFERENCE

[1] Kwang-Fu Li, Tung-Shou Chen, and Seng-Cheng Wu, "Image tamper detection and recovery system based on discrete wavelet transformation," Communications, Computers and signal Processing, 2001 IEEE Pacific Rim Conference on, volume: 1, Aug. Page(s): 164 -167 vol. 1.

[2] M.Wu, and B. Liu, "Watermarking for Image Authentication," Proceedings of IEEE International Conference on Image Processing, Oct. 4-7, 1998, Chicago, Illinois, USA, vol. 2, pp. 437-441.

[3] Tae-Yun Chung, Min-Suk Hong, Young-Nam Oh, Dong-Ho Shin, and Sang-Hui Park, "Digital Watermarking for Copyright Protections of MPEG2 Compressed Video," IEEE Trans. on Consumer Electronics, vol. 44, no. 3, Aug. 1998, pp. 895-901.

[4] C.-Y. Lin, and S.-F. Chang, "Semi-Fragile Watermarking for Authenticating JPEG Visual Content," *SPIE International Conf. on Security and Watermarking of Multimedia Contents II*, vol. 3971, No. 13, EI '00, San Jose, USA, Jan 2000.

[5] C.-Y. Lin and S.-F. Chang, "Issues and Solutions for Authenticating MPEG Video," SPIE International Conf. on Security and Watermarking of Multimedia Contents, vol. 3657, No. 06, EI '99, San Jose, USA, Jan 1999.

[6] C.-Y. Lin, and S.-F. Chang, "A Robust Image Authentication Method Surviving JPEG Lossy Compression," Proc. IS&T/SPIE, San Jose, January 1998.

[7] C.-Y. Lin, and S.-F Chang, "A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation," CU/CTR Technical Report 486-97-19, Dec. 1997.

[8] L. M. Marvel, G. Hartwig, and C. G. Boncelet Jr., "Compression Compatible Fragile and Semi-Fragile Tamper Detection," SPIE International Conf. on Security and Watermarking of Multimedia Contents II, vol. 3971, No. 12, EI '00, San Jose, USA, Jan 2000.

[9] E. J. Delp , C. I. Podilchuk, and E. T. Lin, "Detection of Image Alterations using Semi-Fragile Watermarks," SPIE International Conf. on Security and Watermarking of Multimedia Contents II, vol. 3971, No. 14, EI '00, San Jose, USA, Jan 2000.

[10] N. D. Memon, P. Vora, and M. Yeung, "Distortion Bound Authentication Techniques," SPIE International Conf. on Security and Watermarking of Multimedia Contents II, vol. 3971, No. 15, EI '00, San Jose, USA, Jan 2000.

[11] K. Toyokawa, N. Morimoto, S. Tonegawa, K. Kamijo, and A. Koide, "Secure Digital Photograph Handling with Watermarking Technique in Insurance Claim Process," SPIE International Conf. on Security and Watermarking of Multimedia Contents II, vol. 3971, No. 42, EI '00, San Jose, USA, Jan 2000.

[12] Jiri Fridrich, and Miroslav Goljan, "Images with self-correcting capabilities," Proceedings of 1999 IEEE International Conference on Image Processing, volume: 3,PP. 24 -28 Oct. 1999, Page(s): 792-796 vol. 3.

[13] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," in Proc. IEEE Int. Conf. on Image Processing, Sep. 1996, vol. 3, pp. 243-246.