International Journal of Multimedia and Ubiquitous Engineering
Vol.9, No.6 (2014), pp.219-232
http://dx.doi.org/10.14257/ijmue.2014.9.6.22

Biological Virus Model Based Reversible Video Watermarking

Bong-Joo Jang[1], Suk-Hwan Lee[2*], SangHun Lim[1] and Ki-Ryong Kwon[3]

[1]*Korea Institute of Construction Technology,*
[2]*Dept. of Information Security, Tongmyong University, *Corresponding author*
[3]*Dept. of IT Convergence and Application Eng., Pukyong National University,*

roachjbj@kict.re.kr, skylee@tu.ac.kr, shlim@kict.re.kr, krkwon@pknu.ac.kr*

Abstract

Infectious video watermarking (IVW) is to embed the first watermark in encoder/decoder for the protection of video contents and to infect the watermark in different codecs whenever video contents are copied or edited. This paper presents an infectious reversible video watermarking for fast infection in the infectious watermarking model (IWM). Our method is designed by following main features. The first is that the watermark for the available period of video contents is combined with the control code for content-based video watermarking. This makes the video quality and strength be adaptively controlled in the infectious process. The second is the low complexity for fast infection. The third is to embed the infectious watermark as a unit of macro block (MB) for avoiding the delay time for extracting and recovering. Experiment results verified that the reversible watermark can be detected or recovered without loss in different codecs and the quality of recovered content has maintained in the same bit-rate.

Keywords: *Infectious watermarking, Reversible video watermarking, Copyright protection, Biological virus model*

1. Introduction

Video cryptography performs primarily on compression domain because of high capacity of video contents [1-3]. Thus, the main feature of video cryptography is to improve the encryption efficiency while decreasing the computational complexity. Most of video cryptography techniques encrypt motion vectors, quantized coefficients, or entropy codes of different parameters in the encoding process. These methods make it very difficult to find perceptually the similarity between the encrypted video and the host video. However, although the video can be well encrypted perceptually, the decrypted video by licensed user cannot be guaranteed in safety.

Dissimilar as video cryptography for the access control of video content, video watermarking has been presented for the protection of ownership or copyright of distributed video content [4-9]. Video watermarking can be classified to robust/fragile and reversible/irreversible on purposes of application. These features of each of watermarking types have been well known. Among these watermarking types, the reversible watermarking is to recover the watermarked video content to host video content. It can minimize the degradation of quality. On the other hand, two techniques can be introduced in a view of embedding process. The first is content-based watermarking using video data before compression. The second is the codec-based watermarking using compression parameters like

ISSN: 1975-0080 IJMUE

transform kernel or motion vector in codecs. However, these techniques are very difficult realistically to robust to all of trans-coding, re-compression, or different image processing.

For solving these realistic problems, we introduced infectious information hiding system (IIH) [9] and reversible IIH [17] for the protection of video contents. This system models the relation of video contents and codecs by the relation of biological virus and host organism. It means that IIH infects the watermark under video editing or trans-coding by accomplishing the detecting/mutation/re-embedding process of hidden watermark. The IIH system consists of infectious verification, infectious information generation and management, content-based information hiding, codec-based information hiding.

This paper presents an infectious reversible watermarking for kernel-based information hiding of IIH. The main features of our method are as follows. 1) Our method enables both the quality and the embedding strength to control adaptively using the infectious information with control code and expiration code. 2) Since we hide the watermark plus side information into quantized coefficients in each of MBs, our method has low computation and has no delay time of frames or MBs for recovering original video. 3) Our method can prevent the attack trial because the quality of video will be degraded by the recovery error in attacked video stream. 4) Our method provides video streams of low resolution or low quality when the codec is unauthorized or the video stream is expired. Our experiment verified that our method has no loss of reversible watermark and can preserve the similar quality of general compressed stream without the embedding.

2. Related Works

2.1. Infectious Watermark Model

The hidden watermark in decoded video data should be designed to be robust to video editing, geometric modification, and also compression that is an evitable process for transmitting video data. It is very difficult to design the watermarking that is robust to all attacks of compression, video processing including editing, geometric modification, and frame dropping. In our previous paper, we presented the infectious information hiding (IIH) system that enables to preserve the watermark continuously, regardless of different video attacks. Our IIH system considers the watermark as the virus and the video content as the host organism as following the infectious theory of biological virus and infects the hidden watermark in host video through encoder and decoder. Figure 1 shows the structure and scenario of our IIH system.

IIH system has four techniques of infectious information verification (IIV), infectious information generation and management (IIG), content-based embedding and detecting module (C-EM and C-DM), kernel-based embedding and detecting module (K-EM and K-DM), as shown in Figure 1. We designed the scenario with the assumption that the copyrighter or owner hides the robust watermark (or pathogen watermark) into a host video content. The encoder and decoder of each codec infect the information. The infection process of information in encoder is follows. 1) C-DM that is the previous step of encoding detects the robust watermark in watermarked host video content. 2) IIV verifies this watermark and then IIG regenerates by modifying the watermark. 3) K-EM hides the regenerated watermark into encoded video stream. When the decoder does play or edit watermarked video streams, the watermark verification and regeneration are performed similar as the process in encoder and then K-DM detects the watermark and C-EM re-hides the regenerated watermark.

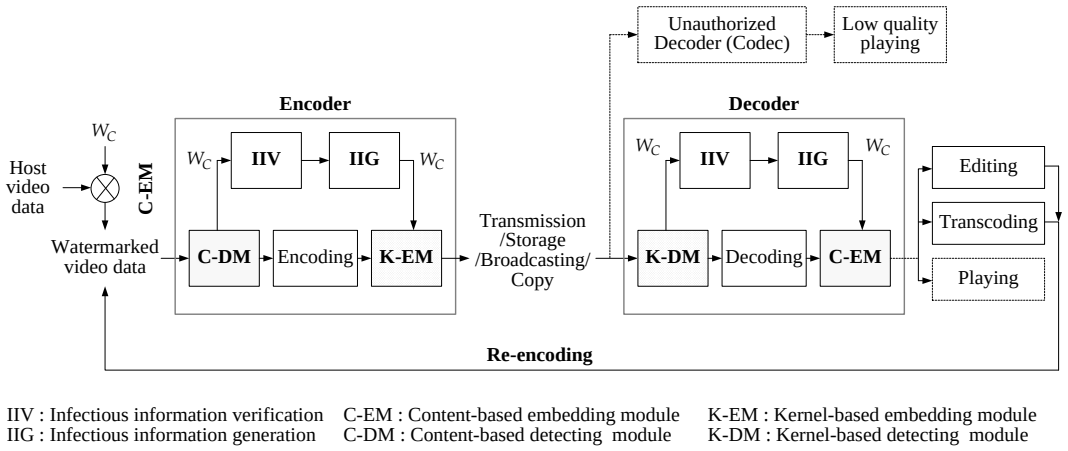


Figure 1. Scenario for Video Content Security in Proposed Infectious Information Hiding (IIH) System

2.2. Reversible Watermarking

Reversible watermarking is a technique that authenticates images and then restores them to original images by removing the watermark. This technique has been mostly designed for applications that are sensitive to the quality degradation. Recently techniques for reversible watermarking have been presented [10-15]. Celik *et al.* [10] compressed bit planes by the lossless compression algorithm and hides the message into empty planes. Thodi *et al.* [11] and Tian [15] proposed difference expansion based reversible watermarking methods.

Most of reversible video watermarking methods have used two properties of histogram and difference expansion. 1) First, histogram based methods have been presented [12-14] by using intensity histogram or intensity difference histogram on different algorithms that lead to low complexity and high capacity. Kuo *et al.* [13] ensured spaces by shifting histogram bins surrounding to maximum point and did shift maximum point to left or right directions on message bits. Yeo *et al.* [14] used the histogram of differences of adjacent pixels. Even if the difference histogram based method uses one maximum point for bit shifting, this method has more high capacity than intensity histogram based method. Therefore, many researchers have used difference histogram for reversible image watermarking. 2) Second, difference expansion based method [15] generates tiny values for describing feature points of image and expands them for hiding reverse data. Hereby, the reverse data is hidden into LSB bits of expanded values. The watermarked image can be regenerated using modified values by the reverse data.

Our previous system [17] does cause the recovery loss of 1 MB/frame, because the additional information of a current macro block (MB) is hidden into a next MB. Furthermore, an error of bits in transmission effects on the video quality because of the relation between watermarks in coded blocks and additional information. This paper presents the reversible video watermarking in infectious information hiding system enable low complexity in the process of encoding and decoding. Hereby, our watermarking enable to control adaptively the embedding strength and invisibility in C-EM (Content based embedding module) step and also enable to degrade intentionally the quality for unauthorized user or decoder in IIG step.

3. Proposed Infectious Reversible Video Watermarking

We introduce a kernel-based reversible watermarking (K-EM and K-DM) and an infectious information management in this section. Infectious information can be used for the copyright or ownership information, the seed number for validate codecs or expiration date, and re-hiding parameters.

3.1. Infectious Information Management

Infectious information hiding systems includes two algorithms of content-based watermarking and kernel-based watermarking that are classified by hidden targets. Accordingly, the types of watermark for infectious information should be modified to be suitable to two algorithms [9, 17]. Our previous method defines two watermarks of pathogen and contagion for C-EM and defines the mutant watermark as the infectious information for K-EM [9].

In this paper, we define newly the infectious information for considering the mutant in reversible watermarking, which becomes the copyright or ownership information and seed number for video authentication. Our method allocates the control codes for different parameters that are required to C-EM and K-EM. Our method hides the expiration data with infectious information. This reason is that we check the system time of decoder using the detected information in intra-frames and then degrade intentionally the quality of intra-frames.

We define the mutant infectious information (MII) by the intra-frame and inter-frame as follows.

$$MII = \begin{cases} (SN(0), t_e, C_A(M, K_A), cc), & \text{if I frame} \\ (SN(f\%gop), C_A(M, K_A), cc), & \text{if P or B frame} \end{cases} \quad (1)$$

$SN(t)$ is the seed number on variable t. If the current frame is intra-frame, the seed number is $SN(0)$, $t = 0$. Or if it is inter-frame, the seed number is $SN(f\%gop)$ depending on both the group of picture (GOP) and the frame number f. This reason is that if any frames are dropped under the decoding process, this codec will be not authenticated. t_e is the system time for representing the expiration data. M is the copyright or ownership information. It is encrypted by symmetry-key encryption module $C_A(M, K_A)$ for preventing the disclosure under the infectious process in Figure 1. If the dispute of video contents happens, the owner obtains the right certification of disputed video contents from the key K_A. cc is the memory size for parameters that control adaptively the embedding strength according to C-EM or K-EM algorithms. While the watermark capacity is varied on different embedding algorithms or video resolutions, the length of M and cc are varied. The encrypted version of MII is generated by the symmetry-key encryption module $C_V(\cdot)$.

$$X = C_V(MII, K_V) \quad (2)$$

The symmetry key K_V is for the encoder and decoder.

The expiration date of video contents should be controlled by K-EM and D-EM. For them, we generate the key k_C using the expiration time t_e and the current system time t_s of codec. This key is used for the watermark embedding and detecting about the seed number of relative frames.

$$k_C = (-1)^u SN(i),\ 0 \le i < gop \quad (3)$$

$$u = \begin{cases} 0, & \text{if } i = 0 \text{ or } t_e - t_s > 0 \\ 1, & \text{otherwise} \end{cases} \quad (4)$$

k_C determines also the positions of watermarks. When video contents has passed the expiration date, it is very difficult to detect the watermark or recover original video contents because the expired video contents generates a different key value to k_C.

3.2. Kernel-based Reversible Watermarking

Our method that is kernel-based reversible watermarking in Figure 1 hides the bits of watermark into selected coefficients that are obtained from DCT and quantization. Hereby the watermark includes side information for recovering video contents in the detecting process. Our method is performed in the previous step of entropy coding in general coding process, which has a series of steps of spatial/temporal prediction, DCT transformation, quantization, scanning, and entropy coding, as shown in Figure 2.

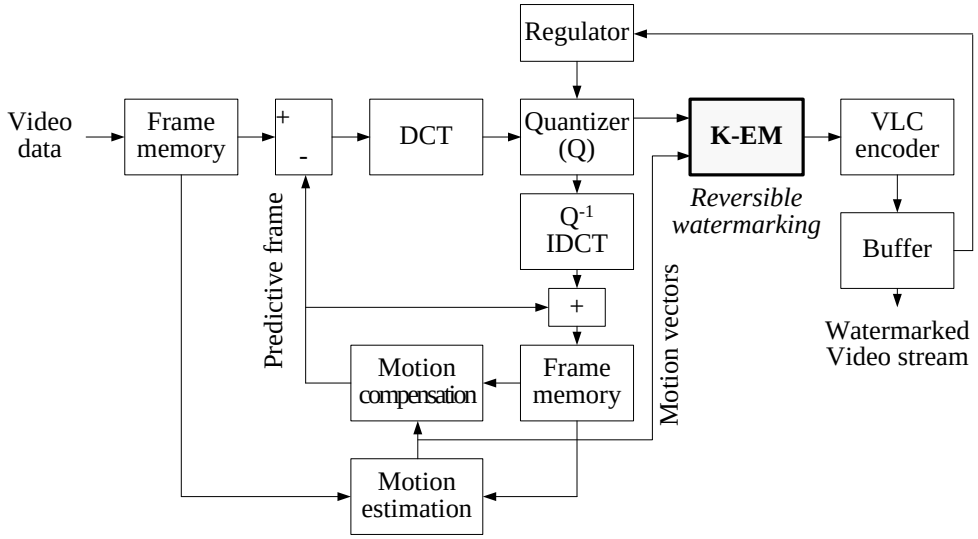


Figure 2. Our Reversible Watermarking (K-EM) Step in General Video Encoding Process

In general video codec, a macro-block (MB) consists of DCT frequency blocks for luminance and chrominance signals. The number of luminance DCT blocks |B| can be determined to four or sixteen according to specific algorithms. To the real-time reversible watermarking in video codec, our method hides a bit of watermark in a DCT block within a MB that is the unit of motion estimation in MPEG2 and AVC codecs. The embeddable blocks B_m^W in mth MB is defined by as follows.

$$B_{m,n}^{\mathrm{W}} = \begin{cases} B_{m,j}, & z_{i,B_{m,j}} \neq 0 \\ NULL, & z_{i,B_{m,j}} = 0 \end{cases}, \text{ for } 4 \leq i < 2^d \quad (5)$$

$$d = \begin{cases} 6, & \text{if } |B| = 4 \\ 4, & \text{if } |B| = 16 \end{cases} \text{ and } \begin{cases} 0 \leq j < \frac{|B|}{2}, & \text{if } seed(R(k_C) + m) = 1 \\ \frac{|B|}{2} \leq j < |MB|, & \text{if } seed(R(k_C) + m) = 0 \end{cases}$$

The unique key value k_C that is generated in encoder and decoder in Equation (3) enables to detect the watermark and to recover original video. Furthermore, it is used for authenticate

the relative codec in infectious information hiding system. From Equation (5), we obtain a seed value of 1-bit using the index of MB m and the random number $R(k_C)$ and determine the embeddable blocks B_m^W. Also, we determine the recoverable blocks B_m^S that correspond to B_m^W as follows.

$$B_{m,n}^{\mathrm{S}} = \begin{cases} B_{m,|B|-j-1}, & z_{i,B_{m,|B|-j-1}} \neq 0 \\ NULL, & z_{i,B_{m,|B|-j-1}} = 0 \end{cases}, \text{ for } 4 \leq i < 2^d \tag{6}$$

We finally determine target blocks $B_{m,n}^T$ in MBs for embedding the watermark and side information using $B_{m,n}^W$ and $B_{m,n}^S$.

$$\boldsymbol{B}_m^{\mathrm{T}} = \{(B_m^{\mathrm{W}}, B_m^{\mathrm{S}}) |\ \forall\, B_{m,n}^{\mathrm{W}}, B_{m,n}^{\mathrm{W}} \neq NULL\} \tag{7}$$

From Equation (7), our method can hide the watermark and side information of $|B_m^T|$ bits.

We select the DCT coefficients in target blocks B_m^T for embedding bits of watermark.

$$f_m^{\mathrm{W}} = First\ NZC\ of\ z_{B_m^{\mathrm{W}}}(j) \text{ and } f_m^{\mathrm{S}} = First\ NZC\ of\ z_{B_m^{\mathrm{S}}}(j) \text{ for } 4 \leq i < 2^d \tag{8}$$

Thus, we obtain scanned values z of coefficients on luminance DCT blocks that are satisfied in Equation (7) and then select first NZC (non-zero coefficient) from fourth scanned coefficient. This reason is that codecs that cannot apply K-EM or is not correspond to k_C enables to decode only low frequency coefficients. These codecs can provide the video stream of low quality.

Given a bit x_i of watermark X in Equation (2), x_i is hidden using the sign of f_i^W in embeddable blocks in Equation (8).

$$f_i^{*\mathrm{W}} = (-1)^{x_i+1} |f_i^{\mathrm{W}}| \tag{9}$$

f_i^{*W} should be recovered to original value f_i^W for the reversible property. The side information s_i is necessary for this reversible property. s_i is determined by checking whether f_i^W is changed or not.

$$s_i = \begin{cases} 1, & \text{if } f_i^{\mathrm{W}} = f_i^{*\mathrm{W}} \\ 0, & \text{if } f_i^{\mathrm{W}} \neq f_i^{*\mathrm{W}} \end{cases} \tag{10}$$

A bit s_i of side information is hidden using f_i^S in recoverable blocks in Equation (8).

$$f_i^{*\mathrm{S}} = (f_i^{\mathrm{S}} \ll 1) + s_i \tag{11}$$

f_i^S corresponds to $\mathrm{f_i^W}$. s_i recovers f_i^{*W} to f_i^W by autonomously detecting.

3.3. Kernel-based Reversible Detecting

The process of kernel-based reversible watermark detecting and video recovery is performed through the reverse process of Figure 2. First, our method decodes a received video stream and finds coefficients into which the watermark and side information are hidden using the key k_C and random generator $R(k_C)$ through Equations (5)-(8). Then, our method detects bits of the side information $\hat{s}_i$ using LSB of entropy decoded coefficients $\hat{f}_i^{*S}$ in recoverable blocks

$$\hat{s}_i = \begin{cases} 1, \text{if } LSB\ of\ \hat{f}_i^{*\mathrm{S}} = 1 \\ 0, \text{if } LSB\ of\ \hat{f}_i^{*\mathrm{S}} = 0 \end{cases} \tag{12}$$

$\hat{f}_i^{*S}$ can be recovered to f_i^S by the reverse process of Equation (11). Hereby, we denote the recovered coefficient as $\hat{f}_i^S$.

$$\hat{f}_i^S = \hat{f}_i^{*S} \gg 1 = f_i^S \tag{13}$$

Finally a bit of watermark can be detected from a coefficient $\hat{f}_i^{*W}$ in embeddable blocks.

$$\widehat{w}_i = \begin{cases} 1, \text{if } \hat{f}_i^{*W} > 0 \\ 0, \text{if } \hat{f}_i^{*W} < 0 \end{cases} \tag{14}$$

And then $\hat{f}_i^{*W}$ can be recovered to $\hat{f}_i^W$ using $\hat{s}_i$.

$$\hat{f}_i^W = (-1)^{\hat{s}_i+1} \hat{f}_i^{*W} \tag{15}$$

4. Experimental Results

In our experiment, we used MPEG2 video codec for evaluating the performance of our reversible watermarking that is based on K-EM and K-DM modules for infectious information. And we used 30 frames of a video sequence with 1280x544@24fps. Figure 3 shows any frame of test video.

Figure 3. A Frame of Test Video Sequence of 1280x544@24fps

4.1. Watermark Capacity

The length of watermark can be determined by adjusting four parameters $(SN(t), t_e, C_A(M, K_A), cc)$ in Equation (1) according to the resolution and compression ratio of relative video sequence. We computed the capacity of watermark of test sequence using the condition of Equation (7) and illustrated the results on Figure 4. From these results, the watermark was hidden into average 2,500 MB/frame among 5440 MB/frame. Thus, the capacity of our watermark is average 2,500 bits/frame. This means that our method has high capacity of watermark.

According to the above results, we generated the mutant infectious information MII of total 512 bits in Equation (1); 256 bits of copyright information M, 64 bits of expiration data t_e, 32 bits of seed number $SN(t)$, and 160 bits of control memory size cc. Then, we generated 512 bits of watermark X encrypting MII by 128-bit DES block-cipher and embedded X repeatedly on capacity of each frame. The repeated times is average four or five.

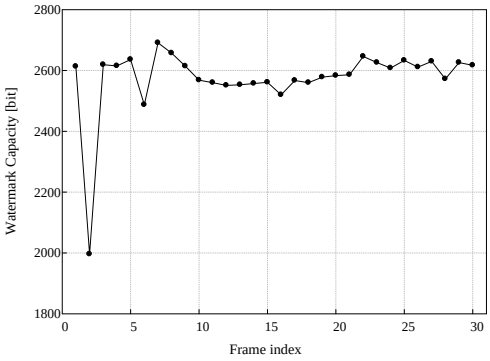


Figure 4. Watermark Capacity of our Method for 30 Frames of Test Video Sequence

4.2. Computational Time

Our method enables to solve two problems of conventional reversible watermarking methods. The first problem is the delay of frame or MBs that occur in the detecting process of side information or the recovery to original video. The second problem is that the watermark should be detected on the reverse of play order. Moreover, our method hides both all side information for the recovery of original video and the watermark in the quantized coefficients in selected MBs. Thus, since the watermark plus side information is hidden in the encoding or decoding processes, the computational time for embedding or detecting is very low. We measured the computational time for K-EM and K-DM in encoding and decoding processes. From experimental results, we know that the encoding and decoding with K-EM and K-DM take delay about 0.003ms/frame and 0.001ms/frame comparing with the encoding and decoding without K-EM and K-DM. This delay time is low for real-time reversible watermarking.

4.3. Attack Analysis

Our designed IIH system detects the watermark while processing the decoder and then infects the watermark using kernel-based reversible watermarking. Therefore, we evaluated the robustness to attacks for compressed video stream excluding attacks for decoded frames. Figure 5(a) shows any frame of recovered video after K-EM and K-DM processing. Meanwhile, Figure 5(b) shows any frame of recovered video after K-EM and K-EM processing and the re-hiding of random watermark that is considered as attack. When collusion attack by different watermarks or watermark removal attack happen to compressed video stream like Figure 5(b), the seed number for hidden positions and key value in Equations (5) and (6) get damaged. The damaged seed number of key value have an effect on degrades of watermark and side information and bring about blocking artifacts. Blocking artifacts that happen sporadically in each frame have a bad effect on video streaming service of high quality. Therefore, we see that our method has a tolerance to attack in compressed stream.

(a) (b)

(c) (d)

Figure 5. Any frame of (a),(b) normal recovered video after K-EM and K-DM and (c),(d) recovered video with the blocking artifacts because of recovery error by re-hiding of the random watermark. ((a),(c) : 25% scaled version of original resolution, (b),(d) : Magnified version of any region)

4.4. Expired Video Stream

We did experiment expired video streams. Thus, when the system time t_s of codec for the watermark detecting or the generating recover key k_C in Equation (3) expired, we blocked high frequency coefficients of the played video stream, into which the watermark and side information are hidden. This enables the expired video stream or unauthorized codec to play only video contents with low quality or low resolution. Figure 6 shows a frame of normalized recovered video stream and a frame of low quality and low resolution in expired video stream or in unauthorized codec. In these figures, we see that expired video stream (or unauthorized codec) has very low quality or low resolution.

4.5. Effect on Compression Ratio

We analyzed the effect of reversible watermark on compression ratio of video stream. When a watermarking method that modifies the compressed stream or quantization table by watermark conforms to the predefined bit rate, the quality of video is degraded. Furthermore, when the watermark changes the coded data in entropy coding step, the increase of the bit rate has occurred and it leads to high quantization parameter in the next quantization step. Since our method hides the watermark in the entropy coding step, as shown in Figure 2, the increase of bit rate and also the degrade of quality have occurred slightly. We computed PSNRs of original video, recovered video, and degraded video like Figures 5(b) and 6(b). These results are shown in Figure 7. As our method uses only sign values of coefficients for the watermark hiding and non-zero coefficients for the side information hiding, the decrease of the entropy coding efficiency has been prevented. Therefore, there are little differences between PSNRs of after and before the information hiding as shown in Figure 7.

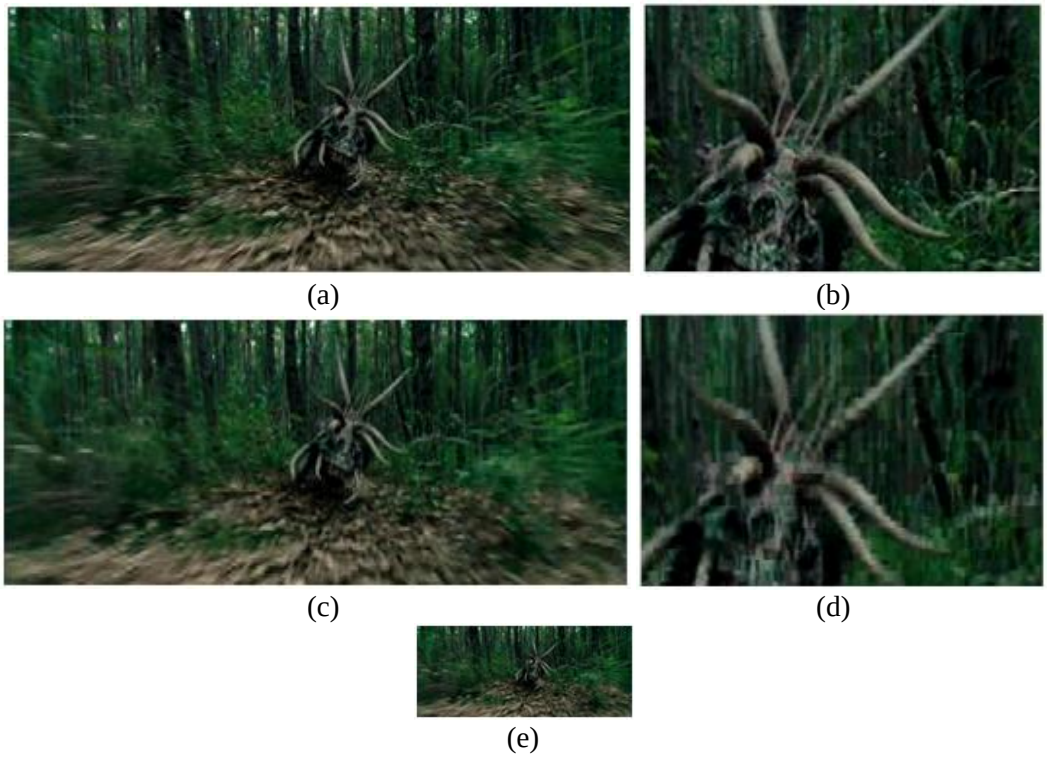


Figure 6. (a)(b) A frame of normal recovered video stream, (c)(d) a frame of low quality in expired video stream or in unauthorized codec, and (e) a frame of low quality and low resolution in expired video stream or in unauthorized codec. ((a),(c),(e) 25% scaled version of original resolution, (b)(d) Magnified version of any region)

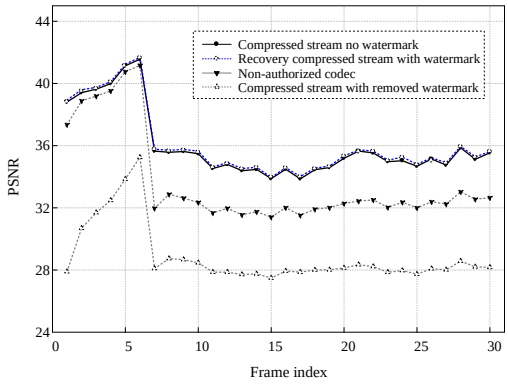


Figure 7. PSNR in Each Frame for Evaluating the Quality by Reversible Watermark

5. Conclusions

We presented an infectious reversible watermarking that infects the reversible watermark with fast and effective in an IIH system for the safe distribution of video contents. Our method can control the video quality and embedding strength adaptively using the control

code and watermark key in the hiding process. The control code is for C-EM algorithm for infecting the watermark. The watermark key is used with the expiration date of video contents. To real-time processing, we hide the watermark into quantized coefficients as a unit of MB and hide the side information for the recovery of original video. Therefore, our method has the advantage of both the low hiding computation and the prevention of frame delay for recovering the original video. Since the video quality can be degraded by the damage of recovery information when compressed video stream is attacked, our method enables the attack attempt to video contents to block. For non-attacked video stream, the loss of watermark is zero after the detection of reversible watermark and the recovery of video. The quality of recovered video is similar to the quality of compressed video with the same bit rate. When the non-authorized codec is used for decoding our watermarked video or the video is expired, our method provides the low quality video with below 30dB PSNR or the low resolution video by removing reversible watermark and performing the de-blocking. That is to enable our method to apply content public relations (PR), free playing service, and other applications. We have improved the content-based reversible watermarking using the reversible watermark and control code with side information and have studied the structure of infectious information and the error correction in IIH system.

Acknowledgements

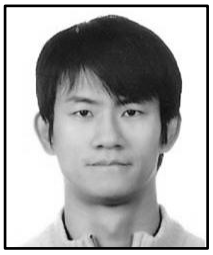
This work was supported under the framework of international cooperation program managed by National Research Foundation of Korea (2012K2A1A2032979) and Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (NRF-2011-0023118) and by a grant from a Strategic Research Project (Operation of Hydrological Radar and Development of a Web-Mobile Warning Platform) funded by the Korea Institute of Construction Technology.

References

[1] B. Furht and D. Kirovski, “Multimedia Security Handbook”, CRC Press LLC, **(2004)**.
[2] A. M. Alattar, “Reversible watermark using the difference expansion of a generalized integer transform”, IEEE Trans. Image Processing, vol. 13, no. 8, **(2004)**, pp. 1147-1156.
[3] J. M. Zain, L. P. Baldwin, and M. Clarke, “Reversible watermarking for authentication of dicom images”, in Proceedings of the 26th Annual International Conference of the Engineering in Medicine and Biology Society, **(2004)** pp. 3237-3240.
[4] A. Mansouri, A. M. Aznaveh, F. Torkamani-Azar, and F. Kurugollu, “A Low Complexity Video Watermarking in H.264 Compressed Domain”, IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, **(2010)**, pp. 649-657.
[5] J. Zhang, A.T. S Ho, Q. Gang, and P. Marziliano, “Robust video watermarking of H.264/AVC”, IEEE Trans. Circuits Sys. Video Tech., vol. 54, no. 2, **(2007)**, pp. 205-209.
[6] E. He, “Video Watermarking Algorithm for Inter-frame Prediction Block Partition Based on H.264 Code”, International Journal of Digital Content Technology and its Applications, vol. 7, no. 3, **(2013)**, pp. 333-340.
[7] M. Jiang, Z. Ma, X. Niu, and Y. Yang, “An Innovative Video Watermarking Scheme Based on H.264 for Copyright Protection”, International Journal of Digital Content Technology and its Applications, vol. 6, no. 5, **(2012)**, pp. 290-297.
[8] J.-S. Yoon, S.-H. Lee, Y.-C. Song, B.-J. Jang, K.-R. Kwon, and M. Kim, “Robust blind video watermarking against MPEG-4 scalable video coding and multimedia transcoding”, Journal of Korea Multimedia Society, vol. 11, no. 10, **(2008)**, pp. 1347-1358.
[9] B.-J Jang, S.-H. Lee and K.-R. Kwon, “Modeling of infectious information hiding system for video contents using the biology virus”, Journal of the Institute of Electronics Engineers of Korea, vol. 49-CI, no. 3, **(2012)**, pp. 34-45.

[10] M.U. Celik, G. Sharma, A. M. Tekalp and E. Saber, "Lossless generalized-LSB data embedding", IEEE Trans. on Image Processing, vol. 14, no. 2, **(2005)**, pp. 253-266.
[11] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking", IEEE Trans. on Image Processing, vol. 16, no. 3, **(2007)**, pp. 721-730.
[12] Z. Ni, Y.-Q. Shi, N. Ansari and W. Su, "Reversible data hiding", IEEE Trans. on Circuits and Systems for Video Technology, vol. 16, no. 3, (**2006**), pp. 354-362.
[13] W.-C. Kuo, D.-J. Jiang and Y.-C. Huang, "Reversible data hiding based on histogram", International Conference on Intelligent Computing, Lecture Notes in Artificial Intelligence, vol. 4682, **(2007)**, pp. 1152-1161.
[14] D.-G. Yeo, H.-Y. Lee, and B. M. Kim, "High Capacity Reversible Watermarking using Differential Histogram Shifting and Predicted Error Compensation", Journal of Electronic Imaging, SPIE, vol. 20, no. 1, **(2011)**.
[15] J. Tian, "Reversible data embedding using a difference expansion", IEEE Trans. on Circuits and Systems for Video Technology, vol. 13, no. 8, **(2003)**, pp. 890-896.
[16] X. Zeng, Z.-Y. Chen, M. Chen and Z. Xiong, "Reversible Video Watermarking Using Motion Estimation and Prediction Error Expansion", Journal of Information Science and Engineering, vol. 27, **(2011)**, pp. 465-479.
[17] B.-J Jang, S.-H. Lee and K.-R. Kwon, "Active video watermarking technique for infectious information hiding system", Journal of Korea Multimedia Society, vol. 15, no. 8, **(2012)**, pp. 1017-1030.

Authors



Bong-Joo Jang, He received B.S. and M.S. degrees in electronic engineering from Busan University of Foreign Studies, and Ph.D. degree in information security from Pukyong National University in 2002, 2004 and 2013 respectively. He visited Colorado State University in USA at 2011–2012 with visiting scholar. He is currently a Postdoctoral Research Fellow in Korea Institute of Construction Technique. His research interests include multimedia compression and security, digital image/video/vector processing and weather radar systems.

Suk-Hwan Lee, He received a B.S., an M.S., and Ph.D. degrees in Electrical Engineering from Kyungpook National University, Korea in 1999, 2001, and 2004 respectively. He is currently an associate professor in Department of Information Security at Tongmyong University and a member of executive committee of IEEE R10 Changwon Section. His research interests include multimedia security, digital image processing, and computer graphics.

Sanghun Lim, He received the Ph.D. degree in Electrical Engineering from the Colorado State University in 2006. Since then he had carried out various researches in radar meteorology and hydrology as research scientist of Colorado State University and NOAA. Currently, he is a research fellow at Korea Institute of Construction Technology and pursuing development of heavy rainfall/snowstorm disaster forecasting and warning platform using hydrological radars.

Ki-Ryong Kwon, He received the B.S., M.S., and Ph.D. degrees in electronics engineering from Kyungpook National University in 1986, 1990, and 1994 respectively. He worked at Hyundai Motor Company from 1986–1988 and at Pusan University of Foreign Language form 1996–2006. He is currently a professor in division of Electronics, Computer, and Telecommunication at the Pukyong National University. He is currently the Editor-of-Chief in Journal of Korea Multimedia Society. His current research interests are in the area of digital image processing, multimedia security and watermarking, wavelet transform.