J Inf Process Syst, Vol.11, No.2, pp.280~294, June 2015
http://dx.doi.org/10.3745/JIPS.02.0013

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Biological Infectious Watermarking Model for Video Copyright Protection

Bong-Joo Jang*, Suk-Hwan Lee**, SangHun Lim*, and Ki-Ryong Kwon***

Abstract

This paper presents the infectious watermarking model (IWM) for the protection of video contents that are based on biological virus modeling by the infectious route and procedure. Our infectious watermarking is designed as a new paradigm protection for video contents, regarding the hidden watermark for video protection as an infectious virus, video content as host, and codec as contagion medium. We used pathogen, mutant, and contagion as the infectious watermark and defined the techniques of infectious watermark generation and authentication, kernel-based infectious watermarking, and content-based infectious watermarking. We experimented with our watermarking model by using existing watermarking methods as kernel-based infectious watermarking and content-based infectious watermarking medium, and verified the practical applications of our model based on these experiments.

Keywords

Biological Virus Modeling, Copyright Protection, Infectious Watermarking, Video Watermarking

1. Introduction

Since 1990, many researchers [1-10] have worked on watermarking and fingerprinting for the copyright and ownership of multimedia contents. However, most of them have not overcome the limitations of data capacity, reliability, and degraded quality. In this paper we will examine the typical watermarking methods that are used on a variety of frequency kernels and video codecs, which are reported to be robust to image processing. Hartung and Girod [1] scanned temporal and spatial signals on decoded video frames to one-dimensional signal and embedded the watermark signal using a spread-spectrum technique. Swanson et al. [2,3] presented an object-based transparent watermarking technique and temporal wavelet transform based multi-resolution watermarking technique. Serdean et al. [4] designed a watermarking algorithm that has the high embedding capacity and geometric robustness on wavelet transform domain. Wang and Pearmain [5] presented a DCT-based watermarking technique that has the geometric robustness under the MPEG-2 compressed stream. Above them, a number of other video watermarking techniques [6-14] have been presented. However, most of the existing techniques have a difficulty in practically commercializing product because of some

Manuscript received May 08, 2014; accepted June 13, 2014; onlinefirst December 31, 2014.
Corresponding Author: Ki-Ryong Kwon (krkwon@pknu.ac.kr)
* Water Resource Research Division, KICT, Goyang 411-712, Korea (roachjbj@kict.re.kr)
** Department of Information Security, Tongmyong University, Busan 608-711, Korea (skylee@tu.ac.kr)
*** Department of IT Convergence and Application Engineering, Pukyong National University, Busan 608-737, Korea (krkwon@pknu.ac.kr)

considerable defects. The watermark that is hidden in the video data before the compression stage can be lost in the process of quantization. Furthermore, it is very difficult to guarantee that the hidden watermark has the robustness in the geometric processing stage, like rotation, translation, and cropping of any frame.

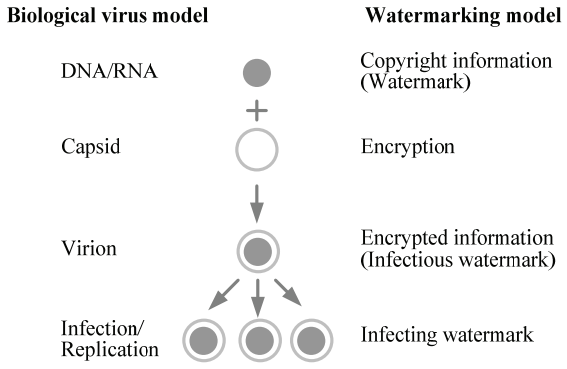

Fig. 1. Modeling of infectious watermarking by using the biological virus theory.

One of the most recent works by Khalilian and Bajic [10] presented a video watermarking method with empirical PCA-based decoding of the wavelet domain. This method embeds the watermark in the LL subband in an adaptive manner that is based on the energy of LL subband wavelet coefficients and visual saliency. They proved that this method is robust to spatial and compression attacks by MPEG-2, H.263, and H.264, and temporal attacks. Cedillo-Hernandez et al. [11] presented a robust video watermarking method that implements video transcoding on the base-band domain. This method employs four criteria based HVSs in the DCT domain and uses the quantization index modulation (QIM) algorithm to embed and detect the watermark in the 2D-DCT domain. Similar to the QIM algorithm, Hasnaoui and Mitrea [12] introduced the framework that allows the binary QIM embedding methods to be extended towards the multiple-symbol QIM for MPEG-4 AVC watermarking. Wang et al. [13] presented a method of video watermarking in a real-time compressed domain with resistance to geometric distortions. The watermarking techniques in the compression domain have been improved by controlling some of the compression parameters, in order to minimize the hidden watermark from being lost in the process of quantization or video editing. However, the hidden watermark can be lost in the re-compression of decoded video data or in the video transcoding by different codecs.

Some of the major problems of conventional video watermarking techniques are as follows: first, watermarking techniques that use a specific codec have not worked well with a variety of video codes [15,16], with their own compression coding methods, nor with standard video codecs [17-23]. Furthermore, they have not worked well with hierarchical compressions like Scalable video coding (SVC) or multiview video coding (MVC) that produce various output streams in a source. Second, video content techniques have progressed and grown exponentially, which creates legal and technical limits for the video watermarking produce. Nevertheless, video content techniques need an integrated copyright protection system that is effective and trustworthy for video content techniques.

This paper proposes an infectious watermarking model using the biological virus theory for a novel paradigm integrated copyright protection system that can handle various video codecs. Thus, the purpose of our watermarking model is to preserve or spread the hidden watermark when video data is

copied or edited on various tools and trans-coded on various codecs. Our watermarking model regards the encoder and decoder of each video codec as an intermediate host and then detects, mutates, and re-hides the hidden watermark, in order to ensure that it is not lost. From the experimental results, we verified that our watermarking concept, which is based on the biological virus theory, is effective for integrated or multiple video codecs.

2. Behind the Infectious Watermarking Model

Our IWM-based video content protection system is based on the idea of how a biological virus works in nature. We previously modeled the infectious information hiding (IIH) system using the biological virus process [14]. However, IIH is only interested in hiding information. In this paper, we design the organization and infectious process of the biological virus as the watermarking theory for protecting video contents.

2.1 Infectious Watermarking Model

We design the infectious watermark regarding as the particle of a biologically infectious virus, which is the priority consideration in our IWM system. Fig. 1 shows our infectious watermark model using biological virus. DNA/RNA, which is the most important genetic material in a biological virus, can be used as the watermark for the copyright and access control of valuable video content. A capsid, which is the nucleic acid surrounded by a protective protein coat, can be used as the encryption and decryption processes that are carried out for protecting the copyright information.

Hence, the combination of DNA/RNA and capsid generates virions of complete virus particle. Viruses can spread as virions from a host under the infectious conditions. Virions can be classified as pathogen, mutant, and contagion according to infectious ways and types. We used the name and concepts of pathogens, mutants, and contagions and then created the infectious watermark by encrypting the copyright information and authority for the video contents from a biological virus.

2.2 Infectious Condition and Infection Process Modeling

The features of infection conditions are as listed below.

- Virus infection and growth has been accomplished by using the process where a virion breaks into a target cell and delivers genetic material to the cell. We modeled our watermarking process after the virus infection and growth process.
- There are many different ways how descendant virions are created different types of cells. These different ways can be used as different watermarking algorithms that are compatible with the different types of contents or codecs.
- When a virus is spread through the cells, hundreds of descendants are reproduced from a virion. This reproduction can be used as the model for re-hiding a hidden infectious watermark in the process of content duplication or trans-coding.
- A biological virus has two ways of lysis and lysogeny for reproduction.
- A biological virus is classified as being a lysis or lysogeny virus in accordance how the infection

properties for reproduction work. The lysis virus that dissolves or destructs a host cell can be used as model for creating the authority code for display devices or decoded video contents.

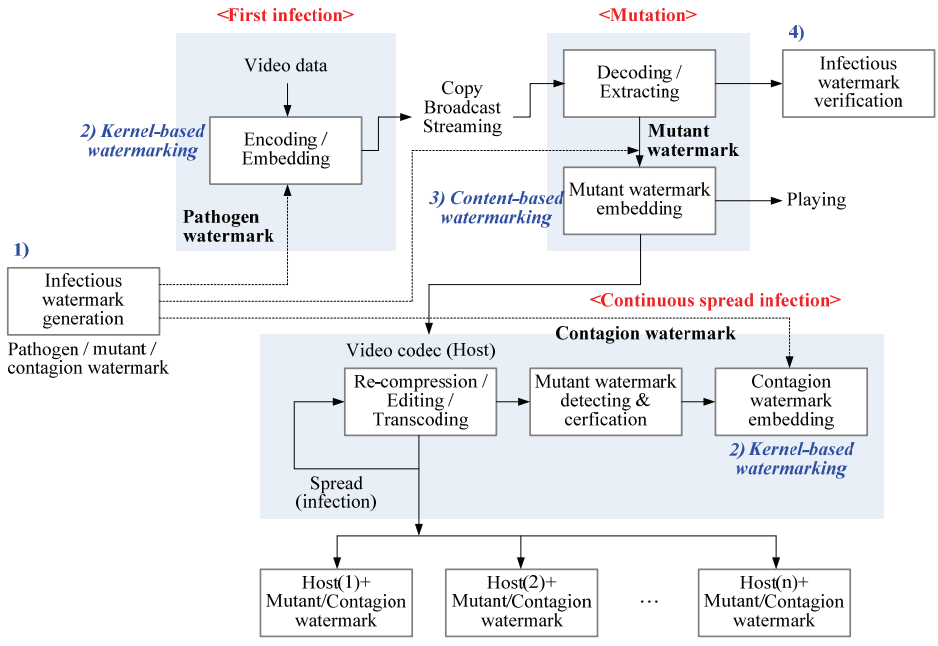

Fig. 2. Descriptive concepts and security strategy for video contents in our watermarking model.

- The lysogeny virus that conceals the genetic material in a host cell until reproduction conditions are met can be used as a model for the copyright protection or authentication of a hidden watermark.
- The infection of virus in a host cell can be used in the infectious watermarking process.
- The ways in which a virus infects its host are different on the structure of the host cell. By viewing a host cell as the video content, the watermarking methods can be worked differently on the type of video contents of video data or of a compressed bit-stream.
- A biological virus is reproduced or spread by infected hosts. We used this concept for designing a method where the infectious watermark can spread throughout all of the video contents that are reproduced or trans-coded.

3. Proposed Infectious Watermarking Technique

Our model focuses on how to design a watermarking system (or integrated system) so that it can handle various codecs. There are not any perfect watermarking methods to robust to the rapid development of codecs and conditions, which anyone can manipulate, edit, and distribute video contents using various codecs. Our model attempts to solve these problems by using a systematic approach that is based on a biological virus infectious model. Thus, our model aims to accurately deliver the watermark in the process of editing, re-compression, and trans-coding. To accomplish this,

our model views various video codecs as being the same as a host in a biological virus infection. It then extracts the watermark in the encoding process and also re-hides the mutant of the watermark in the decoding process. Through our model, the watermark can be continuously embedded into edited, re-distributed, and trans-coded contents by the host codec.

We have defined a new technical description and strategy for an infectious watermarking modeling (see Fig. 2) using the biological virus theory in Fig. 1. Our watermarking modeling has four descriptive concepts in Fig. 2, which are as follows: 1) the generation and management of an infectious watermark (Fig. 2(a)); 2) host-based infectious watermarking (Fig. 2(b)); 3) content-based infectious watermarking under displayed video contents (Fig. 2(c)); and 4) infected watermark verification to checkup on the infection and to control the authority (Fig. 2(d)). Our watermarking model allows many different watermarking techniques to apply for purposes of each descriptive concept. We will define the four descriptive concepts in detail and suggest future research areas for each descriptive concept in the subsections below.

3.1 Infectious Watermarking Generation

This technique is used to generate and manage many different infectious watermarks for the copyright protection or authority management of video contents. The feasible works for infectious watermarking techniques are as follows:

- Cultivation technique for two different infectious watermarks on the type of host
  - Cultivation of the pathogen and contagion watermark in the codec host
  - Cultivation of the mutant watermark in the content host
- Cultivation technique of the watermark for copyright/ownership and authority
  - Reliable cultivation of the watermark from user information
  - Maintain the compatibility between the copyright/ownership and authority in the mutation of pathogens, contagions, and mutant watermarks.

We define the three different watermarks of pathogens, contagions, and mutants, which are used in the infectious watermarking model as described below.

1) The *pathogen watermark* is the infectious information of the producer or copyright owner. It can be used in a cryptography algorithm as the encryption key. In this case, this watermark has the meaning of lysis virus. The pathogen watermark can be infected in macro-blocks of the base layer in a hierarchical video codec like SVC and MVC.

2) The *mutant watermark* is the mutant of the pathogen watermark that is extracted in the decoding process. This watermark can be used in content-based infectious watermarking by using decoded and reconstructed video data. The mutant watermark can be embedded into all of the layers of a hierarchical video codec.

3) The *contagion watermark* is the transfectant of an extracted mutant watermark in the decoding process. This watermark is similar to the pathogen watermark in its properties. A contagion watermark can be embedded in the process of video storing or re-compressing.

Pathogen and contagion watermarks should be discriminated on the infectious process. Just as two capsids of the pathogen and contagion can be different in the infection of a biological virus, the bit-

streams of the pathogen and contagion watermarks can be different for different encryption algorithms. However, they can be generated to same binary information in the way that they are embedded in the video codec.

We generated both the binary information $\mathbf{B}$ of N-bits for copyright or authority and the binary key $\mathbf{K}$ of the same bits using a pseudo-random number generator (PRNG). Then we produced a pathogen watermark $\mathbf{w}^{\mathrm{P}} = \{w_i^{\mathrm{P}} = [0,1]\}$ by combining $\mathbf{B}$ with $\mathbf{K}$ using the XOR operator. Our simulation used the same bit-stream for the pathogen watermark $\mathbf{w}^{\mathrm{P}}$, the contagion watermark $\mathbf{w}^{\mathrm{C}}$, and the mutant watermark $\mathbf{w}^{\mathrm{M}}$ to reduce the simulation complexity.

$$\mathbf{w}^{\mathrm{P}} = \mathbf{w}^{\mathrm{C}} = \mathbf{w}^{\mathrm{M}} = \{w_i = b_i \oplus k_i \mid i = [0, N]\} \tag{1}$$

3.2 Host-Based Infectious Watermarking

This watermarking is used to hide the infectious watermark in the hosts for various video codecs. This means that the infectious watermark in decoded video data does infect again as mutant in the re-compression or trans-coding of video data. The feasible works for host-based infectious watermarking are as follows:

- The infectious watermarking method, which is based on quantization, DCT/DWT kernel, or ME/MC in the encoding process
  - Generation of infected video contents by the pathogen and contagion watermarks
  - DCT/DWT based infectious watermarking in a codec
  - ME/MC based infectious watermarking in a codec
- Reversible infectious watermarking in the certification of authority
- Non-reversible infectious watermarking in the non-certification of authority
  - Content-based encryption is available for the non-reversible infectious watermarking.

Host-based infectious watermarking for injecting a pathogen and contagion watermark should be simple and should be applied to different video codecs. We will now present a host-based infectious watermarking method based on the methods of Kim et al. [9], which is very simple and is applicable to different video codecs, as it only uses parameters in the encoding process.

First, we determined the number of watermark bits R^{W}, which will be periodically embedded on the frame frequency f_{intra} so as to improve the reliability of the watermark. Thus, R^{W} can be defined by the frame frequency f_{intra}, by the bit number of pathogen watermark $|\mathbf{w}^{\mathrm{P}}|$, and by the numbers of DCT blocks in a frame, N_{B}, as follows:

$$R^{\mathrm{W}} = |w^{\mathrm{P}}| \times \lfloor N_{\mathrm{B}} / |w^{\mathrm{P}}| \times f_{\mathrm{intra}} \rfloor \tag{2}$$

As such, we set: f_{intra} =1 and $\mathbf{w}^{\mathrm{P}}$ =64 bits. Second, we calculated the complexity C_n of 4×4 blocks in an intra-frame for considering the invisibility and flexibility of different block sizes. Thus, the block complexity C_n can be defined by DCT coefficients in a high frequency region of Ω, except for the four low frequency coefficients and the DC coefficient.

$$C_n = \sum_{u,v \in \Omega} |x_n(u,v)| \text{ for all } n \in N_B \tag{3}$$

$x_n(u,v)$ is a DCT coefficient on the (u,v) position. We then arranged all of the DCT blocks in descending order of the block complexity C_n and selected N_B^W ($N_B^W < N_B$) DCT blocks from the highest complexity for the embedding blocks. We denoted the rank of block complexity as $rank(C_n)$ and the block index of rth ranked complexity; $r = rank(C_k)$ as $k = rank^{-1}(r)$. Therefore, the indices of the embedding blocks are denoted as:

$$\mathbf{K} = [k_1, k_2, \cdots, k_{N_B^W}] \tag{4}$$

where $k_i = rank^{-1}(r_i)$ and $r_i = rank(C_{r_i}) < r_{i+1} = rank(C_{r_{i+1}})$.

We selected a coefficient of $x_k(u,v)$ in each of embedding block and modified it by a watermark bit.

$$x_k'(u,v) = \overline{C}_k(w_k + \alpha_k) \text{ where } \overline{C}_k = c_k / N_k \text{ for all } k \in \mathbf{K}. \tag{5}$$

N_k is the number of high frequency coefficients of Ω, except for the four low frequency coefficients and the DC coefficient. Thus, N_k is 10 in 4×4 blocks. w_k is a watermark bit for the kth embedding block and α_k is the parameter for controlling the invisibility and the strength.

To further improve the security, we generated the key values $e_k = (e_k(u), e_k(v))$ of horizontal and vertical permutation for each block and permuted the embedded coefficient of $x_k'(u,v)$ with any coefficient in a block via the key values.

$$x_k'(u,v) \leftrightarrow x_k'(e_k(u), e_k(v)),\ 0 < e_k(u), e_k(v) < 4 \tag{6}$$

In the extracting process, the watermark bit can be extracted by using the permutation key values e_k, and the threshold values th_k, as follows:

$$\hat{w}_k = \begin{cases} 1, & \text{if } \hat{x}_k(e_k(u), e_k(v)) \geq th_k \\ 0, & \text{otherwise} \end{cases} \text{ for all } k \in \mathbf{K} \tag{7}$$

We determined the threshold value th_k by the block complexity $\overline{C}_k$ and the number N_k of high frequency coefficients Ω from Eq. (5).

$$th_k = c_k / N_k \tag{8}$$

3.3 Content-Based Infectious Watermarking

This watermarking is used to hide the infectious watermark in the image data of played video contents. It is performed on the primitive video data or decoded video data. The feasible works for content-based infectious watermarking are as follows:

- The generation of an embedded frame in the video contents by the pathogen and contagion

watermarks

- Infectious watermarking in a spatial or frequency domain

- Geometric robust infectious watermarking
- Recovery or regeneration of an infectious watermark that is damaged by an attack
- Intentional degradation in the event of there being a non-certification of the detected watermark in the mutant video contents.

Content-based infectious watermarking is used to embed the watermark into a host video data or decoded video data from different codecs. It should be designed for the adaptive to both different spatial resolutions after trans-coding and the spatial resolutions of H.264SE/MPEG-4 SVC codecs. For considering these purposes, we designed content-based infectious watermarking based on the SVC watermarking method [8], which is robust to H.264SE/MPEG-4 SVC and different video codecs or trans-coding. Our method embeds the first watermark into spatial base layers and embeds the second watermark into spatial enhancement layers using interpolation and the quantization table.

To embed the mutant information, we determined the region of interest (ROI) on the spatial resolution of each frame $f(x,y)$ as:

$$R(i,j) \in f(x,y),\ a \le i \le (a+R_H),\ b \le j \le (b+R_V). \tag{9}$$

R_H and R_V are the horizontal and vertical sizes of the ROI that are determined by the scaling parameter γ $(0<\gamma\le 1)$. a and b are the reference coordinate values of ROI and we transformed the ROI to the DCT domain in each frame.

$$c(u,v)=\frac{2}{\sqrt{R_H R_V}}C(u)C(v)\sum_{i=1}^{R_H-1}\sum_{j=1}^{R_V-1}\cos(\frac{(2i+1)u\pi}{2R_H})\cos(\frac{(2i+1)u\pi}{2R_H})R(i,j) \tag{10}$$

$C(u)$ and $C(v)$ are $1/\sqrt{2}$ if $u,v=0$ and they are 1 otherwise.

We extended the quantization table $Q(m,n)$ $(0\le m,n\le 8)$ for the intra frame in MPEG-2 to the horizontal and vertical size of the ROI by using bilinear interpolation.

$$Q_{\mathrm{ROI}}(u,v)=\begin{cases} Q(m,n), & \text{if } u=m\times l_V,\ v=n\times l_H \\ \left\lfloor \sum_{k=-1}^{1}\sum_{l=-1}^{1}\omega(k,l)Q(u+k,v+l)\right\rfloor & \text{if } u=\lfloor l_V(m+1/2)\rfloor,\ v=\lfloor l_H(n+1/2)\rfloor \\ \vdots & \vdots \\ Q(u,v), & \text{if } u=\tau R_V/2^{n+3}-1,\ v=\tau R_H/2^{n+3}-1 \end{cases} \tag{11}$$

and l_H are $l_V=\left|\tau R_V/2^{n+3}\right|$ and $l_H=\left|\tau R_H/2^{n+3}\right|$. $\omega(k,l)$ is 3×3 weighting random matrix that are generated by normal distribution.

$$\omega=\begin{bmatrix} r(t_{-1,-1}) & 2r(t_{-1,0}) & r(t_{-1,1}) \\ 2r(t_{0,-1}) & 4r(t_{0,0}) & 2r(t_{0,1}) \\ r(t_{1,-1}) & 2r(t_{1,0}) & r(t_{1,1}) \end{bmatrix}/\sum_{k=-1}^{1}\sum_{l=-1}^{1}\omega(k,l) \tag{12}$$

$r(t_{k,l})$ is the random value that is generated by the normal distribution of mean=0.5 and variance=1

with a seed $t_{k,l}$.

The extended quantization table $Q_{\mathrm{ROI}}(u,v)$ was used as a watermark key. We aligned the DCT coefficients $c(u,v)$ of the ROI region by using zigzag scan ordering and quantized them by $Q_{\mathrm{ROI}}(u,v)$. Then we selected 64 coefficients from the low frequency region and embedded the watermark bits into specific bits of quantized DCT coefficients as follows:

$$c'(u,v)=\begin{cases}\lfloor c(u,v)/\alpha Q_{\mathrm{ROI}}(u,v)\rfloor \| (1<<\delta), & \text{if } w=1\\ \lfloor c(u,v)/\alpha Q_{\mathrm{ROI}}(u,v)\rfloor \,\&\,\& \sim (1<<\delta), & \text{if } w=0\end{cases} \tag{13}$$

$\|$ and $\&\&$ are bitwise OR and bitwise AND operators. ~ is the bitwise inverse operator. The quantization scale factor α and the bit-shift δ are determined by considering the embedding strength and invisibility of watermark. We obtained the embedded ROI $R'(i,j)$ through inverse quantization and inverse DCT and combined it with a non-ROI.

The extracting process was performed using the watermark key $Q_{\mathrm{ROI}}(u,v)$, in a similar manner to that of the embedding process mentioned above. Thus, the bits of the watermark in each frame can be detected by checking the δ th bits of quantized DCT $\lfloor c(u,v)/\alpha Q_{\mathrm{ROI}}(u,v)\rfloor$ coefficients as follows:

$$\tilde{w}=\begin{cases}1, & \text{if } (\lfloor \tilde{c}(u,v)/\alpha Q_{\mathrm{ROI}}(u,v)\rfloor \,\&\,\&(1<<\delta),)=1\\ 0, & \text{otherwise}\end{cases} \tag{14}$$

3.4 Infectious Watermark Verification

We checked the embedding of the watermark by using the detecting process when the video contents are encoded or decoded. If relevant video contents are judged to be embedded with the watermark, we extracted the infectious watermark and verified the copyright of ownership or authority from the extracted watermark by using the infectious watermark verification. The related works that should be carried out the infectious watermark verification are as follows:

- The reliable verification technique of extracted infectious watermark
- The creation of the policy for authority control for copying, linking, and editing by using the verified infectious watermark
  - Authority grant technique in the process of encoding and decoding considering codecs or tools as intermediate host in online/offline
  - The creation of protocol or syntax for reliability verification and authority control

4. Experimental Results

Our watermarking model should be followed by further studies for descriptive concepts defined in Section 3. It is expected that existing watermarking techniques will be even more greatly improved if they are reinterpreted and applied to our model. This is why we created infectious watermarking for the novel paradigm protection of video contents. We designed this scenario to verify the practicality of our

model and examined from simulations if the primitive watermark could be entirely embedded into many different video contents.

Most of the SWs for video contents call the library of video codecs in device driver form. Therefore, we uploaded our infectious watermarking algorithms into the encoder and decoder of the codec library. We stored the infectious watermark in a capsid form in the SWs that use infected video contents and then embedded again it into transcoding process. In our simulation, we used the H.264 SE/MPEG-4 SVC codecs as the primitive hosts because this codec is easily available for the trans-coding of decoded video contents and it has good integration and complexity in terms of algorithms. Furthermore, we hid or spread the infectious watermark by using the H.264/MPEG-2 codecs as the contagions. Fig. 3 shows the verification scenario of our proposed model.

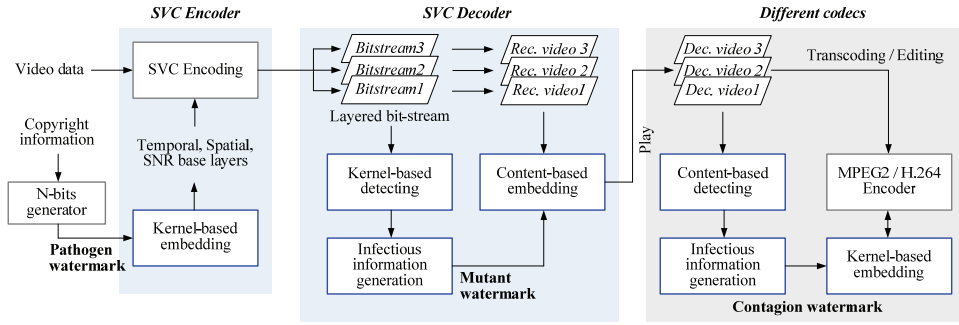

Fig. 3. Simulation scenario of our infectious watermarking.

Fig. 4. Test video sequences: (a) crew (4CIF@30fps), (b) foreman (CIF@30fps), (c) bus (CIF@30fps), and (d) football (CIF@30fps).

We implemented our infectious watermarking model (IWM) using the two techniques of host-based infectious watermarking and content-based infectious watermarking and compared them with the latest methods of Cedillo-Hernandez et al. [11] and Wang et al. [13]. We used the H.264 SE/MPEG-4 SVC as the primary codec for generating the first video content for our implementation, as shown in Fig. 3. This figure shows our scenario for verifying the infectious of watermark in the IWM paradigm. Our experiment verified the infectious of watermark with two strategies. The first is that we decoded the pathogenic video contents with the MPEG-4 SVC and re-coded them with the MPEG-2 codec and then verified the infectious of watermarks in the re-coded MPEG-2 streams. The second is that we trans-coded the re-coded MPEG-2 streams with the H.264 codec and then verified the infectious of the pathogen, mutant, and contagion watermarks. Fig. 4 shows the test video sequences that were used in our experiment.

Table 1. BER results of contagion watermarks in each infectious way in Fig. 3 (the first SVC codec)

Test sequence	Layer	SVC decoded (Host)		
		Proposed (mutant1)	Cedillo-Hernandez et al. [11]	Wang et al. [13]
Crew	4CIF	0.00	0.01	0.05
	CIF	0.00	0.02	0.08
	QCIF	0.00	0.04	0.10
Foreman	CIF	0.00	0.01	0.04
	QCIF	0.00	0.03	0.06
Bus	CIF	0.00	0.02	0.05
	QCIF	0.00	0.03	0.08
Football	CIF	0.00	0.01	0.04
	QCIF	0.00	0.02	0.07

Table 2. BER results of mutant watermarks each infectious way in Fig. 3 (multiple codecs)

Test sequence	Layer	MPEG-2 (1st re-codec)				H.264 (2nd re-codec)			
		Proposed (1st infection)		Cedillo-Hernandez et al. [11]	Wang et al. [13]	Proposed (2nd infection)		Cedillo-Hernandez et al. [11]	Wang et al. [13]
		Encoded	Decoded			Encoded	Decoded		
Crew	4CIF	0.00	0.00	0.02	0.11	0.00	0.00	0.06	0.18
	CIF	0.00	0.00	0.05	0.17	0.00	0.00	0.13	0.26
	QCIF	0.01	0.01	0.11	0.21	0.01	0.01	0.26	0.32
Foreman	CIF	0.00	0.00	0.03	0.08	0.00	0.00	0.06	0.21
	QCIF	0.00	0.00	0.08	0.13	0.00	0.00	0.19	0.31
Bus	CIF	0.00	0.00	0.05	0.11	0.00	0.00	0.13	0.26
	QCIF	0.01	0.00	0.08	0.17	0.01	0.00	0.19	0.31
Football	CIF	0.00	0.00	0.03	0.08	0.00	0.00	0.06	0.21
	QCIF	0.01	0.01	0.05	0.15	0.01	0.01	0.13	0.36

We performed the host-based infectious watermarking on base layers for temporal, spatial, and SNR scalabilities. Different layers in the SVC were encoded to bitstreams independently of each other. The

hidden information in the base layer can be detected in different layers. Therefore, our experiment encoded temporal and SNR scalabilities into one layer in order to avoid complications. We extracted the infectious watermark before and after the different codecs in each of infection ways, as shown in Fig. 3. The results of which are presented in Tables 1 and 2. As can be seen by looking over the results that are shown in these two tables, although the pathogen watermark of 64-bits was infected in encoder and decoder for each of codecs, all of the bits were extracted without bit errors occurring. Furthermore, although the infected watermarks were mutants or re-infected through different infectious ways, most of the bits were extracted without bit errors. However, Antonio's method has a low BER from 0.01 to 0.04 in the first SVC codec. However, it has a high BER from 0.06 to 0.19 in the second re-codec of the MPEG-2/H.264. Similarly, Wang's method has a higher BER than our proposed method and Antonio's method in all test sequences.

Our IWM embedded the pathogen watermark in video codec regardless of the different encoding parameters. We calculated the PSNRs in order to analyze the degraded quality of the infected watermarks in various codecs in Tables 1 and 2. Table 3 shows the PSNRs of different codecs. From this table, we know that the SVC trans-coding of a host video sequence does not degrade the image quality, which is not difference subjectively and objectively and reduce average 3.456 dB. However, the first infection does slightly degrade the image quality which reduces the average PSNR to 5.746 dB. This reason is that the mutant watermark is embedded based on content-based watermarking dissimilarly as the pathogen watermarking and our method considers primarily the robustness. However, extra degradation did not occur after the second infection because of the degeneration and preservation of the infectious watermark.

Table 3. PSNR by infected watermarks in the trans-coding of heterogeneous codecs (dB)

Test sequence	Layer	Host		1st infection		2nd infection	
		MPEG-4 SVC		MPEG-2		H.264	
		Compression	Infection	Compression	Infection	Compression	Infection
Crew	4CIF	41.16	39.41	39.62	35.26	39.50	35.07
	CIF	43.23	40.57	41.45	36.43	41.15	36.44
	QCIF	47.52	42.20	42.12	36.60	42.09	36.45
Foreman	CIF	44.29	41.95	42.54	36.48	42.38	36.30
	QCIF	49.81	44.60	45.07	37.30	45.05	37.23
Bus	CIF	36.52	35.59	32.54	31.41	32.38	31.03
	QCIF	42.05	41.82	37.64	34.31	37.41	34.06
Football	CIF	37.45	35.71	35.68	32.20	35.38	32.08
	QCIF	46.90	41.43	38.59	35.55	38.11	35.52

5. Conclusion

The purpose of our paper was to present a new watermarking system design for the integrated copyright protection system that deals with increased video codecs. The two major contributions of our paper are as follows: 1) we described the IWM for video content protection by modeling the infectious ways and procedure of the biological virus to the watermarking theory; and 2) we introduced the

concept and techniques of our infectious watermarking method. Our IWM views the watermark for video protection to be akin to an infectious virus and the video content and codecs as being the host and contagion medium. We verified the availability of our IWM in the experiments that we conducted, in which we used host-based and content-based infectious watermarking algorithms. Our IWM needs to be improved for the access control of video contents and the robustness to different video processing, for the combination of two or more pieces of video data, and for post-processing. We tried to solve the access control and robustness by using the video editing or recording tools as the contagion medium.

Acknowledgement

This paper was supported by Busan, Korea, under the 2013 Brain Busan 21 program grants and Basic Science Research Program, which are given out via the National Research Foundation of Korea (NRF). The Ministry of Education, Science and Technology (NRF-2011-0023118) fund the NRF. The paper was also supported by a grant from the Strategic Research Project (Operation of Hydrological Radars and the Development of a Web-Mobile Warning Platform), which is funded by the Korea Institute of Construction Technology.

References

[1] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing*, vol. 66, no. 3, pp. 283-301, 1998.

[2] M. D. Swanson, B. Zhu, B. Chau, and A. H. Tewfik, "Object-based transparent video watermarking," in *Proceedings of the IEEE 1st Workshop on Multimedia Signal Processing (MMSP1997)*, Princeton, NJ, 1997, pp. 369-374.

[3] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Multiresolution scene-based video watermarking using perceptual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 540-550, 1998.

[4] C. V. Serdean, M. A. Ambroze, M. Tomlinson, and J. G. Wade, "DWT-based high-capacity blind video watermarking, invariant to geometrical attacks," *IEEE Proceedings Vision, Image and Signal Processing*, vol. 150, no. 1, pp. 51-58, 2003.

[5] Y. Wang and A. Pearmain, "Blind MPEG-2 video watermarking robust against geometric attacks: a set of approaches in DCT domain," *IEEE Transactions on Image Processing*, vol. 15, no. 6, pp. 1536-1543, 2006.

[6] J. Zhang, A. T. S. Ho, Q. Gang, and P. Marziliano, "Robust video watermarking of H.264/AVC," *IEEE Transactions on Circuits Systems II: Express Briefs*, vol. 54, no. 2, pp. 205-209, 2007.

[7] 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, pp. 649-657, 2010.

[8] J. S. Yoon, S.-H. Lee, Y.-C. Song, B.-J. Jang, K.-R. Kwon, M. Kim, "Robust blind- video watermarking against MPEG-4 scalable video coding and multimedia transcoding," *Journal of Korea Multimedia Society*, vol. 11, no. 10, pp. 1347-1358, 2008.

[9] W. J. Kim, T. Y. Seung, S. H. Lee, and K. R. Kwon, "An information security scheme based on video watermarking and encryption for H.264 scalable extension," *Journal of Korea Multimedia Society*, vol. 15, no. 3, pp. 299-311, 2008.

[10] H. Khalilian and I. V. Bajic, "Video watermarking with empirical PCA-based decoding," *IEEE Transactions on Image Processing*, vol. 22, no. 12, pp. 4825-4843, 2013.

[11] A. Cedillo-Hernandez, M. Cedillo-Hernandez, M. Garcia-Vazquez, M. Nakano-Miyatake, H. Perez-Meana,

and A. Ramirez-Acosta, A. "Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT," *Signal Processing*, vol. 97, pp. 40-54, 2014.
[12] M. Hasnaoui and M. Mitrea, "Multi-symbol QIM video watermarking," *Signal Processing: Image Communication*, vol. 29, no. 1, pp. 107-127, 2014.
[13] L. Wang, H. Ling, F. Zou, and Z. Lu, "Real-time compressed-domain video watermarking resistance to geometric distortions," *IEEE Multimedia*, vol. 19, no. 1, pp. 70-79, 2011.
[14] B. J. Jang, S. H. Lee, and K. R. Kwon, "Modeling of infectious information hiding system for video contents using the biological virus," *Journal of the Institute of Electronics Engineering of Korea: Computer Information*, vol. 49, no. 3, pp. 34-45, 2012.
[15] H.264/MPEG-4 AVC (ISO/IEC 14496-10), *Advanced video coding for generic audiovisual services*, 2003.
[16] ISO/IEC JTC1/SC29/WG11/N5231, *MPEG-21 Multimedia Framework*, 2002.
[17] J. Xin, C. W. Lin, and M. T. Sun, "Digital video transcoding," *Proceeding of IEEE*, vol. 93, no. 1, pp. 84-97, 2005.
[18] H.262/MPEG-2 Part 2 (ISO/IEC 13818-2, MPEG-2 Video), *Information Technology – Generic coding of moving pictures and associated audio information, Part 2: Video*, 1994.
[19] ITU-R Rec. H.263, *Video coding for low bit rate communication*, 1996.
[20] ISO/IEC 14496-2 (MPEG-4 Visual), *Information Technology – Coding of audiovisual objects, Part 2:* Visual, 1996.
[21] ISO/IEC JTC1/SC29/WG11/N5231, *Applications and Requirements of Scalable Video Coding N6830*, Palma de Mallorca, Spain, 2004.
[22] BBC opensource, http://www.bbc.co.uk/opensource/projects/dirac/.
[23] Xvid opensource, http://www.xvid.org, Accessed on Oct. 2013.

Bong-Joo Jang

He received the 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 http://orcid.org/0000-0003-4779-2888

He received the B.S., 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. He is currently a research fellow at Korea Institute of Civil Engineering and Building Technology. He worked at Colorado State University and NOAA/CIRA as research scientist from 2006-2012. His research interests include the quantitative precipitation estimation and hydrometeor classification using dual-polarization radar measurements and weather observation using automotive sensors.

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.