Real Time Watermark Embedding/Detecting System for HDTV

*Sang Jin Hahm, *KeunSik Lee, *KenuSoo Park
*Broadcast Technical Research Institute
Korea Broadcasting System
E-mail : cashy@kbs.co.kr

Abstract

High-quality digital broadcasting contents are susceptible to illegal copy and unauthorized redistribution, which makes broadcasters difficult to protect valuable media assets. So, broadcasters and content providers need the technology for copyright protection of professional digital content. Digital watermarking technology is one of the most actively developed solutions for the copyright protection. This paper suggests the requirements of watermarking technology in DTV(Digital TV) environment for copyright protection and shows the developed real-time watermark embedding/detecting system for HD(High Definition)/SD(Standard Definition) video and experimental results of the system against watermark attack tests. Our watermarking system meets the watermarking requirements of invisibility, robustness and security of DTV environment.

I. Introduction

DTV has such merits as high quality video, 5.1 channel digital sound and additional interactive information. So, recently broadcasting stations in many countries are moving from analog to digital. DTV at Korean Broadcasting System(KBS) has been on the air since 2001. The video scheme of KBS terrestrial DTV is HDTV.

With the progress of Information Technology(IT), it is getting easier to copy digital broadcasting contents without degrading video quality and redistribute on and off line. There are various copyright protection technologies like ATSC flag, digital watermarking, Conditional Access System(CAS), Digital Transmission Content Protection(DTCP) and High-bandwidth Digital Content Protection (HDCP). However, until now there is no standard method to protect digital broadcasting contents from illegal copy and redistributing.

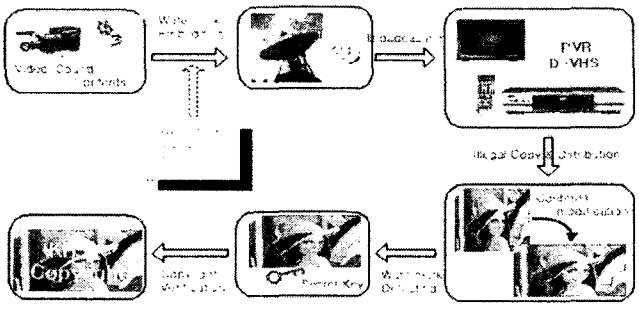

Figure 1. Watermarking scenario in a broadcasting environment

The digital watermarking is to add extra information to digital content and to extract the information in a different environment without additional storage or new format. The original broadcaster is identified by a watermark with copyright information, which enables the detection of illegal copy and unauthorized re-use of contents, as shown in figure 1. This technology is suitable for free terrestrial DTV in a broadcasting environment, which includes all the processes that make, transmit and consume broadcasting contents.

II. Video Watermarking Requirements In A Broadcasting Environment

There are some basic requirements of watermarking system as follows [1].

1. Imperceptibility : The watermark embedding process shall not introduce perceptible artifacts into the original data. Neither visible for image nor audible for sound data.
2. Robustness : The embedded watermark should not be removed by the watermark attack approved by a watermark system.
3. Security : A watermarking system should be secure even if an attacker knows the presence of the watermark. So, the watermarking system usually uses a secret key that is only known to an original contents provider.

2.1 Robustness

A watermark in a broadcasting environment can be used in both production and distribution level. In production level, all the DTV contents are processed

and delivered nearly uncompressed and in distribution level. DTV should be compressed in MPEG-2 format. So, multiple watermarks should be embedded in each level or single watermark which can be detected in both two levels, should be embedded. For the robustness of watermark, a watermark embedded in video is basically designed to survive the MPEG-2 compression attack and still survive various natural or malicious video processing attack such as down or up conversion, filtering, re-sizing, format conversion, AD/DA conversion and cropping.

We propose the watermark attacks and the degree of the attacks to be considered in a broadcasting environment as shown in table 1. We don' t include malicious watermark attacks that degrade video quality under the broadcasting quality.

No	Attack	Description
1	MJPEG Compression	SDTV(20Mbit/s)
2	MPEG-2 Compression	SDTV(2~6Mbit/s), HDTV(19~20Mbit/s)
3	DV Compression	Panasonic/DV, Sony/DV, Sony/Beta-SX
4	Re-Sampling (DA/AD)	DV analog recording
5	Sampling Rate Conversion	Up & Down conversion (SDTV ↔ HDTV)
6	Line-Scan Conversion	Progressive ↔ Interlaced
7	Frame-Rate Conversion	24Hz ↔ 25Hz ↔ 30Hz
8	Aspect-Ratio Conversion	4:3 ↔ 16:9
10	Color-Space Conversion	Color ↔ Gray scale
11	Additive White Noise	At - 30db
12	Slow-Motion	3:1
13	Pixel Shift	Up to half video size
14	Scaling	0.5 ~ 2.5
15	Cropping	Up to half video size
16	Rotate	0 ~ 5°
17	Image Filtering Processing	Character & Graphic insertion, Sharpening, Brightness Up & down, Median filtering (3*3, 5*5), Gaussian filtering and so on

Table 1. Requirements of watermark robustness

2.1 Invisibility and Payload

The measure of video quality can be done subjectively or objectively. The widespread subjective methods are the double-stimulus impairment scale method and the double-stimulus continuous quality scale method of ITU-R BT.500 [2]. The famous objective method is calculating PSNR(Peak Signal to Noise Ratio).

We propose the requirement of video quality that must satisfy over 4 grade of the double-stimulus impairment scale method and over 38 db of PSNR.

A payload of watermark means the size of watermark information. The watermark payload in a broadcasting environment should be over 64 bits for copyright protection [3].

2.3 Security

The watermark can be removed and detected by hostile and malicious attacker. So, the watermarking system protects unauthorized detection and removal of watermark by using secret key. The watermarking system should use secret key in generating, embedding and decoding process. The number of available watermarking secret keys is as large as possible.

Ⅲ. KBS Watermarking System

KBS watermarking system is developed for the copyright verification and protection of KBS DTV contents. The target contents of KBS watermarking system are standard definition video(SMPTE 259M), high definition video(SMPTE 292M) and package media as DVD or VCD.

3.1 Watermarking Algorithm

The information which is embedded into video as a watermark, is 128 bits copyright identifier for HD or SD video. HD-SDI(Serial Digital Interface: SMPTE 292M) or SDI(SMPTE 292M) video signal is composed of Y, Cb and Cr color signal. Our algorithm process only Y signal because Y signal is most robust against various video processing.

3.1.1 Embedding

First, our system extracts Y signal from input video signal. Simultaneously, watermark bits are generated by spread spectrum method with information bits and the secret key. The watermark is embedded in spatial domain of all the sequences. The watermark payload of our system is 128 bits. But, the size of payload can be larger by embedding different watermark on each frame.

Our watermarking algorithm is designed to embed single watermark or multiple watermarks. In case of multiple watermarking, each watermark must be generated by different key and can be detected by each key because the watermark is orthogonal to each other.

The invisibility of watermark is achieved by weakening the strength of watermark. However, it is desirable that the strength of watermark is as high as possible for high robustness. Therefore, the design of watermark strength involves a trade-off between imperceptibility and robustness. Our system calculates the strength of watermark with the luminance and contrast sensitivity of each pixel value to vary according to HVS(Human Visual System). The threshold of watermark strength can be determined to satisfy the requirement of invisibility and robustness in a broadcasting environment after many real empirical tests.

$$\hat{I}_{n,m} = I_{n,m} + \alpha_{n,m} \cdot w_{n,m} \qquad (1)$$

$\hat{I}_{n,m}$: Watermarked Y signal at (n, m)

$I_{n,m}$: Input Y signal at (n, m)

$\alpha_{n,m}$: Calculated watermark strength at (n, m)

$w_{n,m}$: Watermark bit at (n, m)

Equation [1] shows our watermark embedding algorithm. Our watermark embedder adds original Y video signal and coded watermark repeatedly in each video pixel.

3.1.2 Detecting

Our detecting algorithm is divided into two parts- watermark detecting/decoding and affine transform finding. Watermark detecting/decoding is done by correlation method. If decoding doesn' t success, watermark detector estimates affine transform parameter. If there is a geometric watermark attack, watermark detector transforms the video using estimated affine transform parameter.

The watermark detection is designed to be done every second(30 frames) after various watermark attacks listed in table 1. However, under the simple watermark attack, our system can detect watermark in every frame.

3.2 Embedder/Detector

A real time watermark embedder and detector are required for the practical usage in the real broadcasting environment for verification and protection of DTV copyright.

3.2.1 Embedder

The watermark embedder has input/output of SMPTE292M or SMPTE259M signal. Also a RS232 port is provided for changing a watermark message and controlling the embedder by external computer, The whole embedding processing take 1 frame delay.

3.2.2 Detector

We develop real-time watermark detector as PC card type to use in a PC or workstation instead of stand alone type.

Now our watermark detector detects 10 or 12 watermarks in a second under no watermark attack. We will develop the watermark detector that can detect watermark in a second under various watermark attacks.

3.3 Test Environment

The testbed for robustness of watermark is established under considering the real broadcasting environment and illegal redistribution condition, as shown in figure 2. A variety of attacks are tested by two-step. MPEG-2 compression attack is always first performed, and then the others such as image processing filtering, geometric transformation, scan conversion, color-space conversion and cropping are tested.

The invisibility of watermark is measured subjectively and objectively. The subjective invisibility test of watermark is done by " Double stimulus impairment scale method" . The objective invisibility test of watermark is done by calculating the PSNR and picture quality measurement tools, PQA300 of Tektronix [4]. This picture quality analysis tool is based on subjective picture quality tests of ITU-R.BT500.

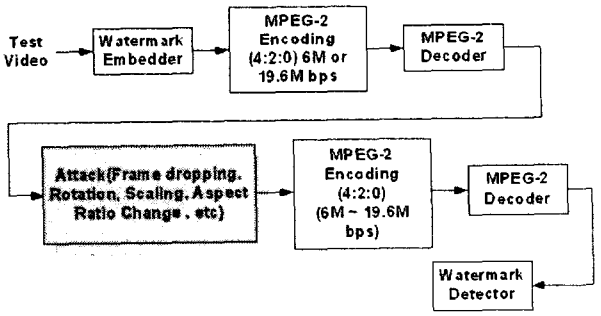

Figure 2. The testbed for watermark robustness

3.4 Test Results

The test sequences are composed of MPEG test videos(SD video,1800 frames, 60 seconds, 6 scenes) and KBS test videos(HD video, 17400 frames, 580 seconds, 30 scenes). Each test sequence is selected according to various features of moving picture(color, line or edge, texture, graphics, object or camera movement).

The robustness of watermark is tested in two steps. Robustness against the first compression for transmission is tested, and then robustness against various attacks is tested after first compression and de-compression. The results of detecting watermark in SD video and HD video after the first MPEG-2

compression(6Mbps for SD, 19.3Mbps for HD) attack are over 95%. The figure 3 shows the result of detecting watermark in SD video under second compression and decompression. As the second compression rate is higher, the detection rate is getting lower. The result of detecting watermark in HD video after compression attack is similar to the result of SD video, as shown in figure 4. However the result of detecting watermark in HD video is lower than that of SD video, because the strength of watermark in HD video is decided weaker than that of SD video for better video quality.

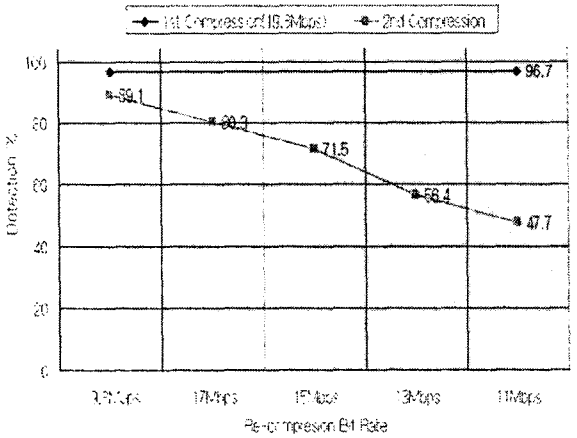

Figure 3. Test result of re-compression attack (SD video)

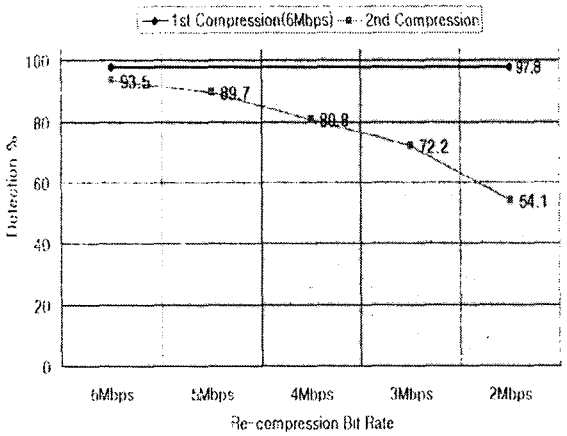

Figure 4. Test result of re-compression attack (HD video)

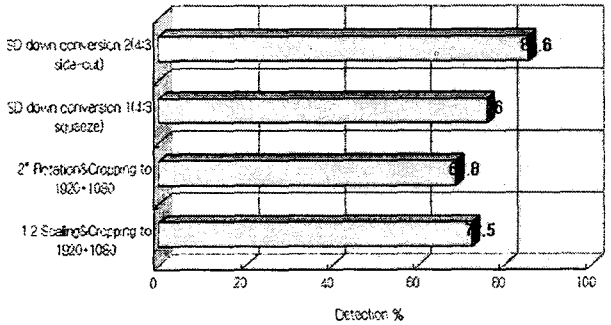

Figure 5. Test result of mixed geometric attacks (HD video)

The figure 5 is the results of detecting watermark after other attacks like cropping, aspect-ratio change, rotation and so on after the first compression, which shows lower detecting result than the first compression attack, but still satisfies the requirements of watermarking in a broadcasting environment.

Ⅳ. Conclusion

A free terrestrial DTV broadcasting company cannot prohibit copying contents for private backup by CAS or other method. However, for copyright protection or contents identification, the terrestrial DTV broadcasting company must prevent other broadcasting companies from illegal use of contents for their interest by identifying contents' owner. The watermarking technology is considered as the most practical and robust copyright protection method for free terrestrial DTV because it is weak and passive way to only insert a logo of broadcasting company into video.

In this paper, we propose the requirements of video watermarking in a broadcasting environment, watermark embedding/detecting algorithm and real-time watermark embedder/detector. The suggested algorithm and requirements are for protecting the copyright of high quality video for broadcasting, not for the low quality video such as low quality Internet streaming video. So the results of test are shown good under the prior condition and our algorithm also suggests enough many bits watermark payload to be used for many applications such as metadata.

We are currently improving the performance of developed watermark embedder and detector in order to extend the field of practical use.

References

[1] I.J. Cox, M.L. Miller and J.A. Bloom, 2002, Digital Watermarking, London:Morgan Kaufmann Pub.

[2] Rec. ITU-R.BT.500-8. 1998, Methodology for subjective assessment of the quality of television pictures. ITU, Geneva, Switzerland.

[3] L.Cheveau, E.Goray and R.Salmon. Watermarking-summary results of EBU test. In EBU technical review, March 2001.

[4] http://www.tek.com/site/ps/0,,25-11735-INTRO_EN,00.html, 2004.