특집논문-05-10-2-01

Real-Time HD Watermarking System in DTV environment

Sangjin Hahm[a)‡], Keunsik Lee[a)] and Keunsoo Park[a)]

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.

Keywords : media assets, digital watermarking, copyright protection, Digital TV, high definition, standard definition

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 KBS(Korean Broadcasting System) has been on the air since 2001. The video scheme of KBS terrestrial DTV is HDTV.

With the progress of IT(Information Technology), it is getting easier to copy digital broadcasting contents without degrading video quality and redistribute on and off line.

There are various copyright verification and protection technologies.

① Encryption/decryption such as CAS(Conditional Access System).
② Copy protection such as DVD CCI(Copy Control Information)
③ Broadcast Flag and digital watermarking.
④ Digital transmission protection such as DTCP(Digital Transmission Content Protection) and HDCP (High-bandwidth Digital Content Protection).
⑤ Fingerprinting

However, until now there is no standard method to protect digital broadcasting contents from illegal copy and redistributing.

The digital watermarking is to add extra invisible or inaudible information to digital content and to extract the information in a different environmentwithout 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

a) Broadcast Technical Research Institute Team Korea Broadcasting System

is suitable for free terrestrial DTV in a broadcasting environment, which includes all the processes that make, transmit and consume broadcasting contents.

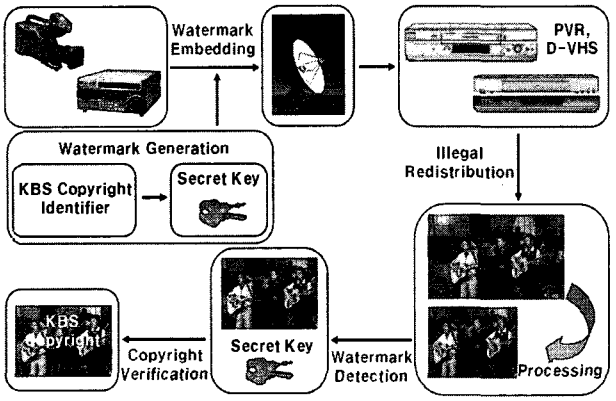


Fig. 1.Watermarking scenario in a broadcasting environment

Ⅱ. DIGITAL WATERMARKING

materials such as video, image, sound and document are duplicated easily and the copy has the same quality as the original. So, the digital watermarking has gained a lot of attention and evolved very fast since the first publication of digital watermarking in 1990 [1].

The basic structure of watermarking process is shown in figure 2. A watermark which is changeable according to the status of a secret key is embedded in the original data invisibly. A watermark attack is all the processes that prevent watermark detector from detecting the watermark or decoding the message of the watermark during the transmission of contents. So, even if there is illegal use including the watermark attack, the watermark must be detected to identify digital contents owner.

There are some basic requirements of digital watermarking as follows [2].

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 anattacker knows the presence of the watermark. So, the watermarking system usually uses a secret key that is only known to an original contents provider.

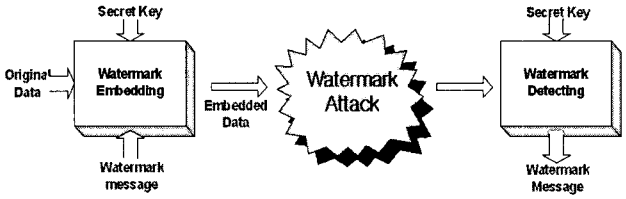


Fig. 2. Watermarking process

Ⅲ. REQUIREMENTS IN DTV ENVIRONMENT

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, format conversion, and AD/DA conversion. We also designed our watermark to survive geometric transform attacks such as resizing and aspect ratio change because HD video can be illegally distributed in resized SD video.

We propose the watermark attacks and the degree of the attacks to be considered in a broadcasting environment as shown in table 1. We propose the watermark detection rate should be over 80% after the attacks listed in table 1. We don't include malicious watermark attacks that degrade video quality under the quality for broadcasting.

2. Invisibility and Payload

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.

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 [3]. 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 in subjective video quality test and over 38 db of PSNR in objective test.

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 [4].

3. Security

Awatermark 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.

Table 1. Requirements of watermark robustness

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

Ⅳ. KBS WATERMARKING SYSTEM

KBS watermarking system is developed for the copy-

right 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.

1. Watermarking Algorithm

1.1 Watermark generation

The information which is embedded into video as a watermark, is 128 bitscopyright identifier for HD or SD video. The information is also called watermark payload. The watermark bits are composed of the information bits and synchronization bits. The synchronization bits are watermark synchronization information that can be used in watermark detection process to find the position of watermark. The sync bits are also used to decide how and how much geometrical transform attacks are done.

The watermark bits are spreaded by M-ary modulation and added ECC(Error Correcting Code) for robustness and security of watermark. We use LDPC(Low Density Parity Check) code as ECC.

And last, for the security of watermark, the position of watermark bits are permutated by secrete key.

1.2 Embedding

HD-SDI(Serial Digital Interface: SMPTE 292M) or SDI(SMPTE 259M) video signal is composed of Y, Cb and Cr color signal. Our algorithm processes only Y signal because Y signal is most robust against various video processing.

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

If input video signal is present, Y signal is extracted from input video signal. Simultaneously, watermark bits are generated by spread spectrum method with information bits and the secret key.

The strength of watermark is calculated 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.

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

$\hat{I}_{n,m}$: Watermark ed 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)

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

1.3 Detection

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

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.

2. Embedder/Detector

A real time watermark embedder and detector arerequired for the practical usage in the real broadcasting environment to verify and protect DTV copyright.

2.1 Embedder

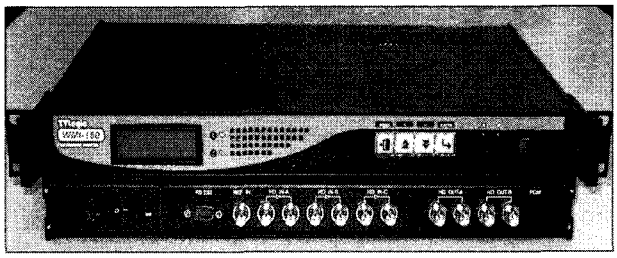


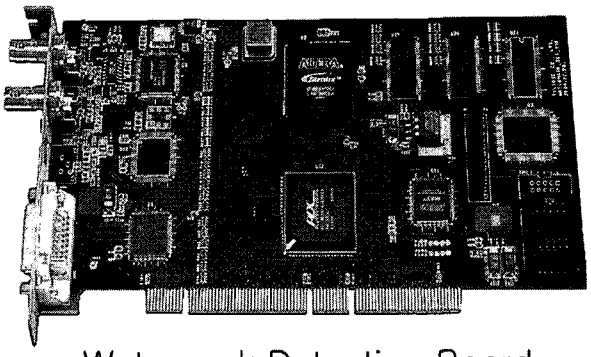
Fig. 3. Real-time watermark embedder

The watermark embedder has interfacesof SMPTE292M or SMPTE259M signal. Also a RS232 port is provided for changing a watermark message and controlling the embedder by external computer, as shown in figure 3. The whole embedding process takes 1 frame delay.

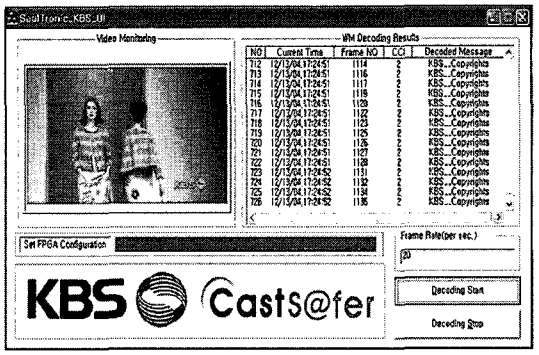
2.2 Detector

We developedreal-time watermark detector as a PC card type to use in a PC or workstation instead of a stand alone type. The figure 4shows the real-time watermark detector we developed. There are two reasons why the watermark detector isdeveloped as a PC card type. The first reason is that a PC card type can be used for many applications such as monitoring advertisement and broadcast which needs a log file. The second reason is that watermark detection process needs more computing power than watermark embedding process does. In case of using detector in a PC, we can use both FPGA processing power of detector and CPU processing power of PC.

Now, our watermark detector detects 30 watermarks in a second. Actually, the watermark detector detects 23~24



Watermark Detecting Board



Watermark Detector S/W UI

Fig. 4. Real-time watermark detect board and S/W UI

watermarks in a second becausewatermark detector uses 6 or 7 frames for the preview of input video as shown in figure 4. Watermark detection ratio can be varied according to CPU processing power, PCI bandwidth and PCI clock.

3. Test Environment

The testbed for robustness of the watermark system is prepared under considering the real broadcasting environment and illegal redistribution condition, as shown in figure 5. A variety of attacks aretested 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

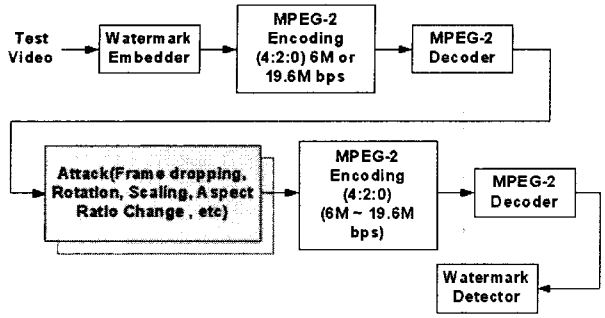


Fig. 5. The testbed for watermark robustness

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"as shown in figure 6. The objective invisibility test of watermark is done by calculating the PSNR and picture quality measurement tools, PQA300 of Tektronix (5). This picture quality analysis tool is based on subjective picture quality tests of ITU-R.BT500.

Fig. 6. The subjective test for invisibility

4. Test Result

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).

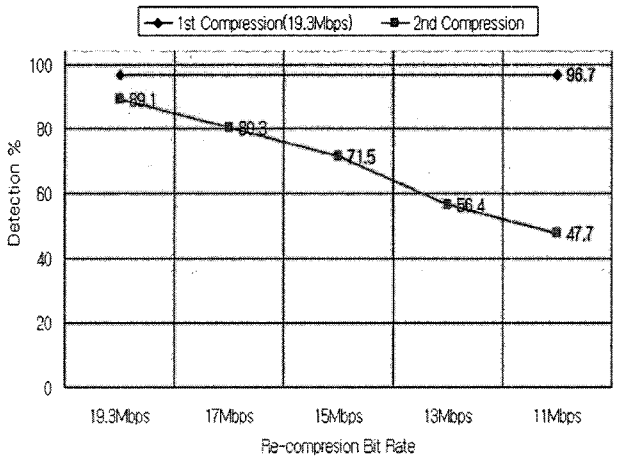


Fig. 7. Test result of re-compression attack (SD video)

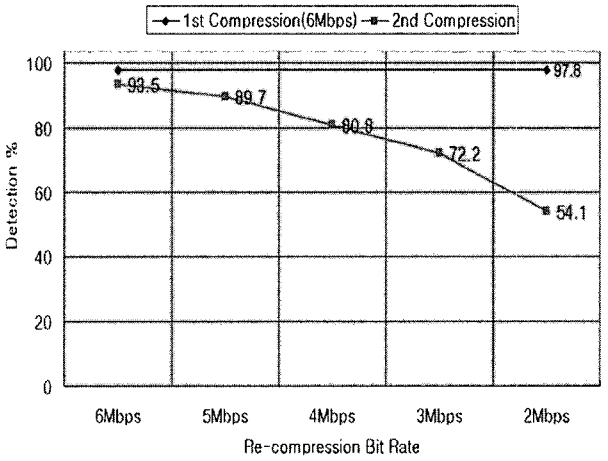


Fig. 8. Test result of re-compression attack (HD video)

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 7 shows the result of detecting watermark in SD video un-

der secondcompression 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 8. 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.

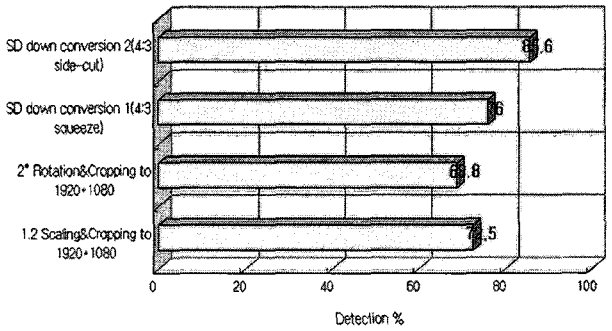


Fig. 9. Test result of mixed geometric attacks (HD video)

The figure 9 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.

Recently, illegally copied contents are easily distributed on the Internet as streaming video that is compressed by streaming codecs like Divx, WMV, Mov and so on. The

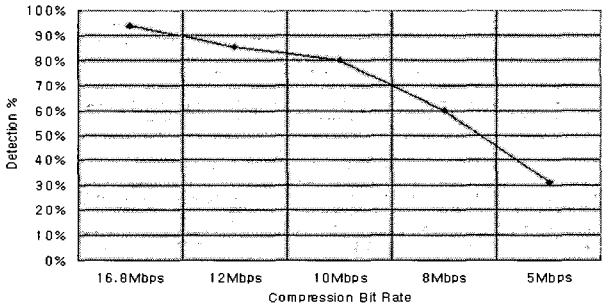


Fig. 10.Test result of compression attacks of WMV(1920*1080i)

streaming codec uses low bit rate compression method. So, a compression by streaming codec is more difficult attack than MPEG compression. The figure 10 is the result of watermark detection after WMV(Windows Media Video) 9 compression. The test result shows lower detecting result than that of MPEG-2 compression. In case of HD(1920*1080i), 19Mbps MPEG-2 video shows the similar quality of 10Mbps WMV video. Our algorithm shows over 80% detection rate in the test of 10Mbps WMV.

V. 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] K.Tanaka, Y.Nakamura, and K.Matsui. 1990, Embedding secret information into a dithered multilevel image. In IEEE Military Commun. Conf., pages 216~220.

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

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

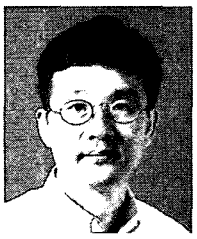
[4] L.Cheveau, E.Goray and R.Salmon. 2001, Watermarking-sum mary results of EBU test. In EBU technical review.11

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

저 자 소 개

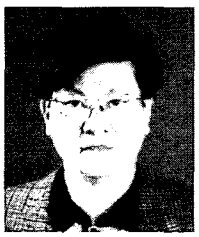
SangJin Hahm

He received BS, MS degrees in Electronic engineering from Yonsei University in 1996, 1998 respectively. He joined KBS (Korea Broadcasting System) in 2001. Since then he has been with KBS Technical Research Team, engaged in the research on video watermarking and intellectual property protection technology



Keunsik Lee

He received BS, MS degrees in Control & Instrumentation engineering from Seoul National University in 1985, 1987 respectively. He joined KBS in 1988. Since then he has been with KBS Technical Research Team, engaged in the research and development of broadcasting equipments.



Keunsoo Park

He received BS degree in Control & Instrumentation engineering from Seoul National University in 1982 and MS degree in electronic and electrical engineering from Korea Advanced Institute of Science & Technology (KAIST) in 1984. He joined KBS in 1984. Since then he has been with KBS Technical Research Team, engaged in the research and development of broadcasting equipments.