SCENE-BASED WATERMARKING METHOD FOR COPY PROTECTION USING IMAGE COMPLEXITY AND MOTION VECTOR AMPLITUDE

Yeong Kyeong Seong, Yoon-Hee Choi**, and Tae-Sun Choi***

* Software Center, Corporate Technology Operations, Samsung Electronics Co., LTD.
Apgujeong Bldg., 599 Shinsa-dong, Gangnam-gu, Seoul 135-893, Korea
** Department of Mechatronics, Kwangju Institute of Science and Technology,
1 Oryong-dong, Buk-gu, Kwangju 500-712, Korea

ABSTRACT

In this paper we propose a new watermarking method based on scene segmentation for copy protection in the hard disk drive embedded digital broadcast receivers. First, video sequence is segmented as scenes using the macroblock types of B-picture in the MPEG compressed domain. Second, for each scene, different embedding parameter is determined from the image complexity and motion vector amplitude. For copy protection, copy control watermark information is embedded in the content whether the content is copyrighted or not. By using this method, invisibility and robustness of watermark, which are the basic requirements of watermark, are satisfied at the same time.

1. INTRODUCTION

As the digital broadcasting is developing, enormous digital multimedia contents are available easily. The availability of multimedia contents in digital forms has brought copyright protection issues of intellectual properties. Digital media have an advantage that can be copied without loss in quality but it is also a disadvantage in the viewpoint of copyright management. There are several researches of copy protection in DVD (Digital Versatile Disk) recorder [1-3].

New platform that embeds hard disk drive in the DBR (Digital Broadcast Receiver) system is developed recently [4]. This system can cause a copyright infringement problem if there is no copy protection scheme. Once a scrambled program is descrambled, this stream can be copied several times after saving in the hard disk drive. So there is a need to add copy protection information to the stream. This information must be strongly embedded to the contents. It can only be removed when the contents suffer severe degradation. This is a reason why watermarking method should be used. For copy protection, watermark information must be embedded in the content and detected whether this content is copyrighted or not. Watermarked video data has two kinds of copy control information i.e., 'Copy never', or 'Copy freely'. When the users try to copy a stream to another media, after checking this copy control information, the copy process is done when the bit is 'Copy freely'. In the case of 'Copy never', the content cannot be copied anymore.

For real-time video watermarking, several methods are proposed [5-6]. G. C. Langelaar et al proposed a video watermarking scheme performed in compressed domain based on VLC codeword [5]. Watermarking in VLC domain is much sensitive to attacks of pirates. M. K. Swanson et al. proposed scene-based video watermarking algorithm using multi-resolution video analysis [7]. The video sequence is segmented into scenes, and temporal wavelet transform is applied to each video scene. This method embeds watermark based on the scene. However, this cannot be applied to real-time application because of its computational complexity.

In this paper, we propose a new copy protection scheme with scene-based watermarking. First, video data is segmented into meaningful scenes using a scene change detector [8] and watermark is embedded as a unit of these scenes. We use different watermark embedding strengths from the image complexity and motion vector amplitude. This method can reduce a computation for parameter determination. Using this method, a reasonable detection ratio and invisibility are obtained.

2. SYSTEM OVERVIEW

To embed and detect the copy protection information, a watermark embedder and detector are added in the DBR. Figure 1 shows the block diagram of the hard disk drive embedded DBR with watermark embedder and detector. If the program is scrambled, the descrambler makes data descrambled. If the user wants to record a program, the data in the buffer is stored in the HDD through the scene change detector and watermark embedder. When the user wants to play the recorded program which is watermark embedded, the data is read from the HDD, checked for the copy protection information, and sent to the MPEG decoders. Besides audio and video data, header position information is also stored in the file for scene-based video watermarking. When the user tries to copy a stream to another media, the watermark detector detects the copy control information to protect an illegal copy.

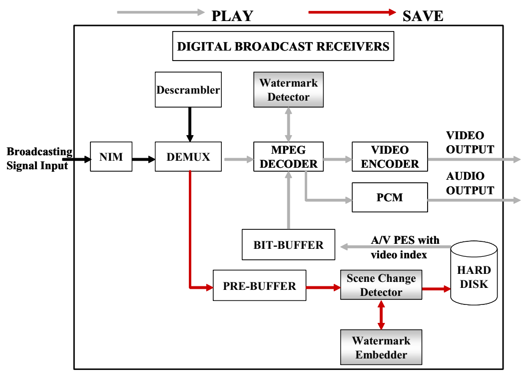


Figure 1. System Overview

3. WATERMARK EMBEDDING AND DETECTION

3.1. Watermark embedding

Watermark embedding process is shown in figure 2. The original video stream is decoded by the variable length decoder (VLD) to separate MB (MacroBlock) type and quantized DCT (Discrete Cosine Transform) image. The scene change detector uses the MB type information to detect the scene change position and the motion vector amplitude is obtained for each MB. The quantized DCT image is inverse quantized and image complexity is calculated. From the image complexity and motion vector amplitude, the watermark embedding factor is decided for adjusting the strength of watermark embedding. We use different watermark embedding strength from the image complexity, i.e., high factor is used for complex scene and low factor is used for monotonous scene. Watermark is embedded in the DCT domain using spread spectrum method, quantized, and re-encoded by the variable length encoder.

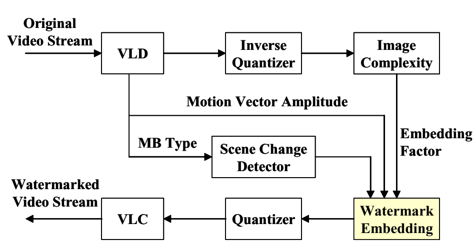


Figure 2. Watermark embedding process

3.2. Watermark detection

Figure 3 shows the watermark detection and copy protection decision process. Watermarked video stream is decoded and inverse quantized by the variable length decoder and inverse quantizer. From this DCT image, watermark is detected. By detecting the watermark, copy protection information is decided.

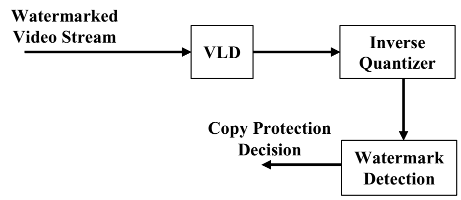


Figure 3. Watermark detection and copy protection decision process

4. SCENE CHANGE DETECTION AND SCENE-BASED WATERMARKING

4.1. Scene change detection algorithm

To make a video index, we use a scene change detection algorithm in the compressed domain using the information of MB type in B-picture for temporal video segmentation. This algorithm is as follows: In the B-picture, the number of interpolated MBs with forward and backward motion compensated (N*INT*) is proportional to the correlation of previous and next I-picture or P-picture. This means that if the number of interpolated MBs is less than a threshold, we can say that a scene change occurs. If a scene change occurs in the small GOP, the MB type of motion compensation of B-picture is dominant for forward or backward motion compensation. This results in the larger difference between the number of MBs with forward and backward motion compensated (N*DIF*) than a threshold. If the number of backward motion compensated MBs of the first B-picture (N*B1*) and the second B-picture (N*B2*) is larger than a threshold, a scene change occurs at the first B-picture because these B-pictures are motion compensated from the next I-picture or P-picture. Otherwise, the number of forward motion compensated MBs of the first B-picture (N*F1*) and the number of backward motion compensated MBs of the second B-picture (N*B2*) is larger than a threshold, we can say that a scene change occurs at the second B-picture. Finally, the number of forward motion compensated MBs of the first B-picture (N*F1*) and the second B-picture (N*F2*) is larger than a threshold, a scene change occurs at the next I-picture or P-picture. Figure 4 shows the basic concept of scene change detection using B-picture type.

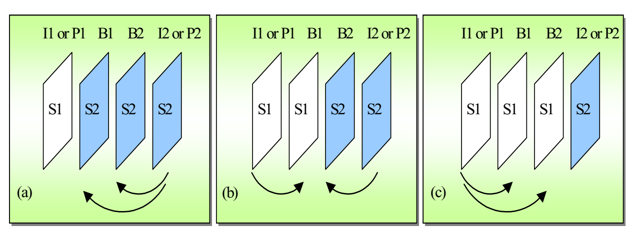


Figure 4. Scene change and MB Type for B-picture

4.2. Scene-based watermarking

The scene-based watermarking approach has an advantage that watermarks can be embedded according to the characteristics of the scene. And video sequences are usually edited as a unit of scene. One scene has similar characteristics because frames in the same scene have similar objects and background. First, video data is divided into meaningful scenes using a scene change detector and watermark is embedded as a unit of these scenes. We use different watermark embedding strength according to the image complexity. Image complexity is calculated from the AC coefficients of DCT image.

$$IC = \sum_{(i,j)=}\sum_{\{i,j|(i,j)\in A\}} \left|DCT(i,j)\right| \qquad (1)$$

,where A={(0,1), (0,2), (0,3), (0,4), (1,0), (1,1), (1,2), (2,0), (2,1), (3,0), (4,0)} as shown in figure 5 (a). From these image complexity measures we determine the watermark embedding parameter. High factor is used for complex scene whereas low factor is used for monotonous scene. The following algorithms determine this embedding parameter α.

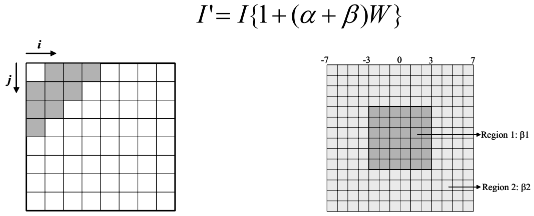
If (scene change has occurred)
    Complexity of Image is calculated;
    If (Complexity of Image > Minimum Complexity)
        α = Const $\times$ Complexity of Image;
    Else
        α = Const $\times$ Minimum Complexity;
Else
        Already calculated α is used;
End

If the motion vector amplitude MV are as follows;

$$\text{If } |MV| \le T_\beta \text{ then } \beta = \beta 1$$
$$\text{else } \beta = \beta 2 \qquad (2)$$

,where $\beta 1$ and $\beta 2$ are parameters for $\beta 1$ and $\beta 2$ region respectively in figure 5 (b). Finally, watermark embedding strength is determined from these two parameters.

$$I' = I\{1 + (\alpha + \beta)W\} \qquad (3)$$



(a) Image complexity (b) Motion vector amplitude
Figure 5. Block analysis

Figure 6 shows the scene-based watermarking method. The block analysis is done only for the fist picture of the scene change. This can reduce the computation of watermark embedding as compared to the conventional method, which computes edge information or block energy for every block for block analysis. This increases a computational complexity of watermark embedding. To reflect a characteristic of each block, motion vector information is used in the block analysis

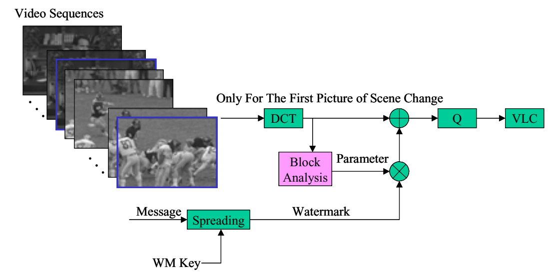


Figure 6. Scene-based watermarking method

5. SIMULATION RESULTS

Simulation is performed to test the performance of the algorithm. We use two kinds of video sequences. One is a simulated video sequence consisting of several standard image sequences. The other is a real broadcasting video sequence captured from the broadcasting. The simulated video sequence is composed of 9 standard image sequences with 2309 frames with size of 352×288. This image sequence is encoded by MPEG-2 encoder. The real broadcasting video sequence is composed of 3000 frames with size of 320×240 and MPEG-2 compressed.

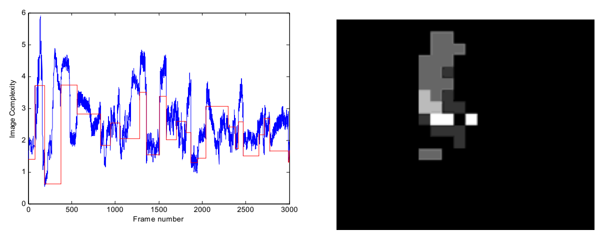
Figure 7 shows the watermark embedded video sequences. Figure 8 (a) shows the image complexity calculated by AC coefficient. Lined plot is α-factor used in the scene for adjusting watermarking strength. Figure 8 (b) shows the region classified by the motion vector amplitude. Figure 9 (a) is watermark detection results for watermarked video sequence. As shown in the results, watermark embedding is invisible with reasonable detection performances.

To evaluate robustness of proposed algorithm, various attacks which are generally applied to digital image watermarking are applied to video sequences. Figure 9 (b)-(f) shows detection results after additive Gaussian noise, low-pass filtering, median filtering, histogram equalization, and resize attacks respectively.

(a) Frame #1: original image (b) watermark embedded image for simulated video sequence

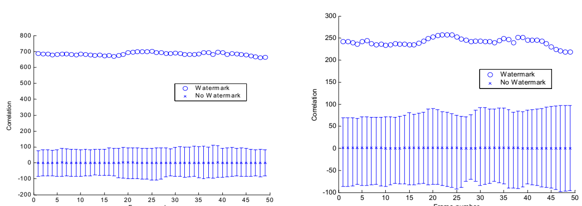
(c) Frame #900: original image (d) watermark embedded image for real broadcasting video sequence

Figure 7. Watermark embedded video sequences

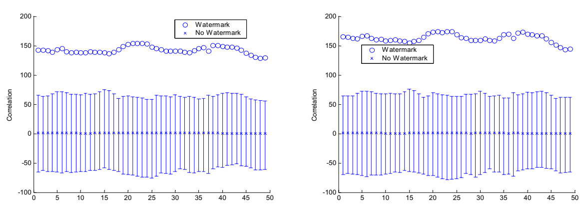


(a) (b)

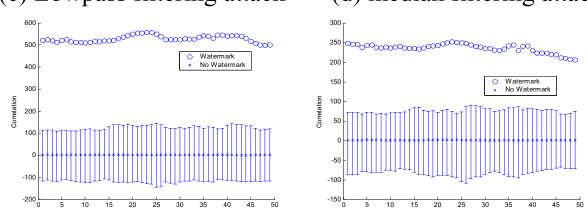
Figure 8. (a) Image Complexity for each scene (b) region classified by the motion vector amplitude



(a) Without attack (b) Gaussian noise attack



(c) Lowpass filtering attack (d) median filtering attack



(e) Histogram equalization attack (f) Resize by 1/2 attack

Figure 9. Watermark detection results for various attacks

Table 1. Watermark Detection Ratio

Total number	Actual		Detected		Detection rate (%)	
	Simulated	Real	Simulated	Real	Simulated	Real
Frames	2309	3000	-	-	-	-
Watermark	2309	3000	2309	2946	100	98.2
Scene changes	9	26	9	24	100	92.3
False alarms	-	-	0	0	0	0

6. CONCLUSIONS

We have proposed a new copy protection scheme with scene-based watermarking. First, video data is divided into meaningful scenes using a scene change detector and watermark is embedded as a unit of these scenes. We use different watermark embedding strength according to the image complexity and amplitude of motion vector. Using this method, reasonable detection ratio and watermark invisibility are obtained. Robustness against various attacks is also investigated. Scene-based watermarked stream can facilitate copy protection. This method can also be applied to illegal copy tracing, called fingerprinting. Contents owner can use fingerprint to track the origin of illegal copied contents. In this case, contents owner can find the users who infringe license agreement and distributes contents illegally by embedding different watermarks such as ID or serial number from users who are provided contents.

7. REFERENCES

[1] J. A. Bloom, I. J. Cox, T. Kalker, J. -P. M. G. Linnartz, M. L. Miller, and C. B. S. Traw, “Copy protection for DVD video,” *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1267-1276, 1999.

[2] M. Maes, T. Kalker, J. -P. M. G. Linnartz, J. Talstra, F. G. Depovere, and J. Haitsma, “Digital watermarking for DVD video copy protection,” *IEEE Signal Processing Magazine*, Vol. 17, No. 5, pp. 47-57, 2000.

[3] C. Busch, W. Funk, and S. Wolthusen, “Digital watermarking: from concepts to real-time video applications,” *IEEE Computer Graphics and Applications*, Vol. 19, No.1, pp. 25-35, 1999.

[4] Y. K. Seong, Y. H. Choi, and T. S. Choi, “Design and implementation of hard disk drive embedded digital satellite receiver with file management,” *IEEE Transactions on Consumer Electronics*, Vol.48, No.1, pp.125-130, February 2002.

[5] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, “Watermarking Digital Image and Video Data,” *IEEE Signal Processing Magazine*, Vol. 17, No. 5, pp. 20-46, 2000.

[6] C. S. Lu, J. R. Chen, H. Y. M. Liao, and K. C. Fan, “Real-time MPEG2 Video Watermarking in the VLC Domain.” *Proceedings of 16th International Conference on Pattern Recognition*, Vol. 2, pp. 552 –555, 2002.

[7] M. K. Swanson, B. Zhu and A. H. Tewfik, “Multiresolution Scene-Based Video Watermarking Using Perceptual Models,” *IEEE Journals on Selected Areas in Communications*, vol. 16, no. 4, May 1998.

[8] Y. K. Seong, Y. H. Choi, J. A. Park, and T. S. Choi, "A hard disk drive embedded digital satellite receiver with scene change detector for video indexing," *IEEE Transactions on Consumer Electronics*, Vol. 48, No. 3, pp. 776-782, August 2002.