

# 장면단위의 비디오 워터마킹을 이용한 복사방지기술

성영경, 최윤희, 최욱철, 최태선  
광주과학기술원 기전공학과

## Copy protection technology using scene-based video watermarking

Yeong Kyeong Seong, Yoon-Hee Choi, Wook-Chul Choi, and Tae-Sun Choi  
Department of Mechatronics  
Kwangju Institute of Science and Technology  
E-mail : sygnus@kjist.ac.kr

### Abstract

디지털 방송의 발달과 인터넷의 사용증가로 인해 멀티미디어 데이터가 기하급수적으로 증가하고 있다. 본 논문에서는 디지털 데이터의 쟁점 중 하나인 불법 복제로부터 저작권을 보호하기 위한 비디오 워터마킹 방법을 제안한다. 하드디스크를 내장한 디지털 방송 수신기에 복사 방지를 위한 복사제어 정보를 장면단위로 영상의 복잡도와 움직임 벡터의 크기를 고려하여 워터마크의 형태로 삽입한다. 즉, 복잡한 장면에 대해서는 강도를 강하게 삽입하고 단순한 장면에 대해서는 강도를 약하게 삽입함으로써 워터마크의 비가시성과 강인성을 동시에 만족할 수 있다.

### I. 서론

디지털 방송이 발전하면서 엄청난 양의 디지털 멀티미디어 데이터가 손쉽게 이용 가능해졌다. 디지털 매체는 질적 손실 없이 복사되는 이점이 있긴 하지만 이는 저작권의 보호 측면에 있어서는 단점이라 할 수 있다. 최근에 디지털 방송 수신기에 하드디스크를 내장한 새로운 플랫폼이 등장하였다 [1]. 이러한 시스템은 일단 스크램블이 해제되면 하드디스크에 저장된 정보를 제한 없이 복사 할 수 있기 때문에 저작권 침해 문제를 일으킬 수 있다. 따라서 방송 스트림에 복사방지 정보를 삽입할 필요가 있다. 이 정보는 콘텐츠에 강하게 삽입되어서 콘텐츠가 심하게 훼손되었을 경우에만 지워져야 하기 때문에 워터마킹 방법을 사용해 삽입하는 것이 적당하다. 개인적인 목적으로 텔레비전 방송을 시간 변환 재생 (Time-shift play)을 위해 저장하는 것은 불법복제행위가 아니다. 그러나, 저작권 보호를 위해 이 방송 데이

터는 한번 저장된 이후에는 더 이상 복제 되어서는 안 된다. 이를 위해 복사제어 정보를 삽입하고 검출하기 위한 워터마크가 필요하다. 워터마크로 들어갈 복사제어 정보에는 'copy never' 와 'copy freely' 의 두 가지가 있다 [2-4]. 비디오 데이터에서 이 복사제어 정보를 확인하여 그 정보가 'copy never' 인 경우에는 복사가 금지된다. 사용자가 스트림을 다른 매체로 전송하려는 경우, 복사제어 정보를 확인한 뒤 이 값에 따라 복사과정을 실행하거나 금지시킬 수 있다.

본 논문에서는 장면전환에 기초한 비디오 워터마킹 방법을 이용한 새로운 복사방지 방법을 제안한다. 먼저 장면 전환 검출 방법을 사용하여 비디오 데이터를 의미 있는 장면단위로 나누고 영상의 복잡도와 움직임 벡터의 크기에 따라 워터마크의 강도를 조절하여 삽입한다 [5]. 이 방법으로 워터마크의 검출과 비가시성의 입장에서 우수한 성능을 얻을 수 있다.

### II. 시스템 개요

하드디스크를 내장한 방송수신기는 기본적인 방송 수신기에 하드디스크와의 정보 전달을 위한 인터페이스가 추가된 형태이다. 복사방지 정보를 삽입하고 검출하기 위해서 방송수신기에 워터마크 삽입기와 검출기가 포함된다. 그림 1 은 하드디스크를 내장한 방송수신기에 워터마크 삽입기와 검출기가 포함된 시스템의 블록도이다. 전송 매체로부터 수신된 방송데이터는 NIM (Network Interface Module) 블록을 통과하여 복조되고 디지털 신호로 변환된다. 이 신호는 하나의 스트림에 여러 프로그램을 포함하고 있다. 사용자가 선택한 하나의 프로그램은 DEMUX 에 의해 분리되어 내부 버퍼에 보내진다. 만약 프로그램이 스크램블 되어 있으면, Descrambler 에서 스크램블을 해제한다. 사용자가 프로

그램을 녹화하려는 경우 버퍼 내에 있는 데이터는 장면 전환 검출기와 워터마크 삽입기를 통해 하드디스크에 저장된다. 그렇지 않으면 압축체계를 위해 MPEG 디코더로 바로 전송된다. 저장하려는 채널에 스크램블이 걸려 있다면 복사 방지 정보는 'Copy never' 이고 무료채널이면 복사 방지 정보는 'Copy freely' 이다. 사용자가 저장된 프로그램을 재생하고 싶을 때에는 하드디스크로부터 데이터를 읽어 들여 MPEG 디코더로 보내진다. MPEG 디코더는 MPEG PES (Packetized Elementary Stream) 의 압축을 풀고 데이터를 비디오 인코더와 PCM 을 통해 각각 TV 화면과 스피커로 보낸다. A/V 데이터의 헤더 위치 정보도 장면기반 비디오 워터마킹을 위해 파일형태로 저장된다. 만약 사용자가 스트림을 다른 매체로 복사하려 하면 워터마크 검출기가 불법 복사를 막기위해 복사제어 정보를 검출한다.

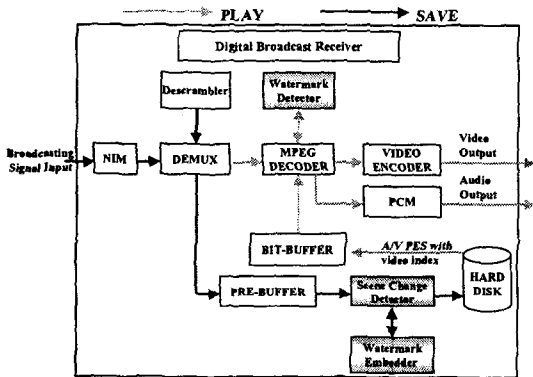


그림 1. 시스템 개요

### III. 워터마크의 삽입 및 검출

워터마크를 삽입하는 과정은 다음과 같다. 원본 비디오 스트림은 VLD 를 이용하여 복호되어 매크로블록 (MB: Macro-Block)의 타입과 양자화된 DCT가 얻어진다. 장면 전환 검출기는 MB 타입 정보를 사용하여 장면 전환 위치를 검출한다. 양자화된 DCT 영상은 역 양자화되고 영상의 복잡도를 계산한다. 영상의 복잡도에 따라 워터마크의 삽입강도를 조정하는  $\alpha$ 값이 결정된다. 복잡한 화면에는 강한 삽입 강도를, 단조로운 화면에는 약한 삽입 강도를 사용한다. 워터마크는 DCT 영역에서 대역확산방법을 이용해 삽입되고 양자화, VLC 를 거쳐 다시 부호화된다. 워터마크를 검출하기 위해 워터마크가 삽입된 비디오 스트림은 VLD 와 역 양자화에 의해 복호화되고 역 양자화된다. 최종적으로 DCT 영역에서 상관도를 계산하여 워터마크를 검출하고 복사 방지 여부를 결정한다.

### IV. 장면전환 검출 및 장면단위 워터마킹

장면단위의 워터마킹은 장면의 특징을 이용하여 워터마크를 삽입하는 방법이다. 대부분의 경우에 비디오 열은 장면 단위로 편집된다. 하나의 장면은 유사한 물체와 배경을 가지므로 유사한 특성을 가지고있다. 먼저, 장면 전환 검출기를 이용하여 비디오를 분할하고 이렇게 분할된 장면을 단위로 하여 워터마크를 삽입한다. 그림 2 는 장면기반 워터마크의 개념을 설명한다.

장면 전환의 검출은 계산을 간략화 하기위해 B-픽처의 MB 타입을 이용한다. 그림 3 에서와 같이 GOP (Group of Pictures)의 일부에서 장면전환이 발생하는 경우는 세 가지의 경우가 있다. 첫번째 경우는 장면전환이 B1 에서 발생하는 경우이다. 이때 대부분의 MB 타입은 역방향 움직임 보상이다. 두 번째 경우는 장면전환이 B2 에서 발생하는 경우이다. 이 경우에는 장면전환이 발생하는 지점 앞뒤에서 움직임 보상 방향이 반대이다. 마지막 경우는 장면전환이 I2 또는 P2 에서 발생하는 경우이다. 이때는 MB 타입이 순방향 움직임 보상이다. 장면전환은 위에 기술한 방법에 따라 MB 타입 정보를 이용하여 검출한다.

분할된 비디오 데이터에는 장면 단위로 워터마크가 삽입된다. 영상의 복잡도는 DCT 영역에서 AC 계수로부터 계산된다.

$$IC = \sum_{(i,j) \in A} \sum_{(i',j') \in A} |DCT(i, j)| \quad (1)$$

, 여기서 A 는 그림 4(a)의 영역으로 나타낼 수 있다.

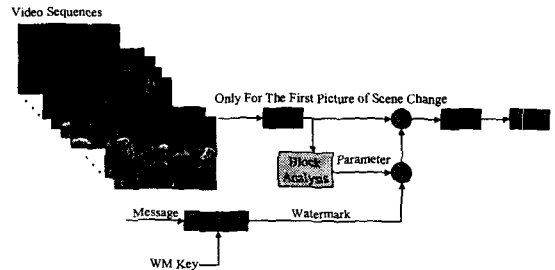


그림 2. 장면 기반 비디오 워터마킹

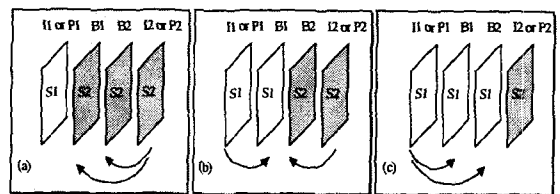


그림 3. 장면전환과 B-픽처의 MB타입

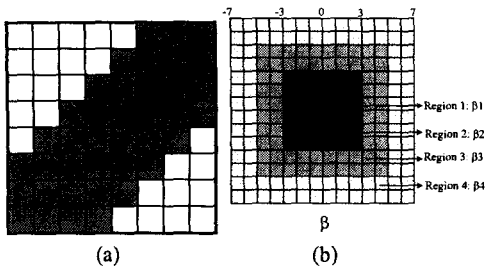


그림 4. 블록 분석

다음은 워터마크 삽입계수를 결정하는 과정이다

```

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

움직임 벡터의 크기 MV가 다음과 같을 때  $\beta$ 는 다음과 같이 결정된다.

$$\begin{aligned}
 & \text{If } |MV| \leq T_{\beta 1} \text{ then } \beta = \beta 1 \\
 & \text{Else if } |MV| \leq T_{\beta 2} \text{ then } \beta = \beta 2 \\
 & \text{Else if } |MV| \leq T_{\beta 3} \text{ then } \beta = \beta 3 \\
 & \text{else } \beta = \beta 4
 \end{aligned} \tag{2}$$

여기서  $\beta 1, \beta 2, \beta 3$  과  $\beta 4$  는 그림 4(b)의 각각 영역  $\beta 1, \beta 2, \beta 3, \beta 4$  의 계수이다. 최종적으로 워터마크 삽입 강도는 다음과 같이 두 계수로부터 결정된다. 즉, 복잡하고 움직임이 많은 부분에는 큰 값이, 단순하고 움직임이 적은 부분에는 작은 값이 사용된다.

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

### V. 모의실험 및 결과

입력 영상은 표준 비디오 시퀀스를 붙여 만든 'simulated' 영상과 실제의 방송을 캡처해서 만든 'real' 영상을 사용한다. 그림 5는 'simulated' 영상시퀀스의 영상 복잡도를 보여준다. 그림 6은 원본 영상과 워터마크가 삽입된 비디오 시퀀스이다. 그림 7은 움직임 보상을 수행한 후의 프레임 차이와 움직임 벡터크기의 범위에 따라 분할될 영역을 보여준다. 그림에서 밝은 부분은 움직임이 많은 부분이고 어두울수록 움직임이 적은 부분이다. 그림 8 과 표 1 은 워터마크 검출 결과이다. 결과에서 보여주듯 워터마크의 비가시성과 검출성능에서 만족스러운 결과를 얻을 수 있다.

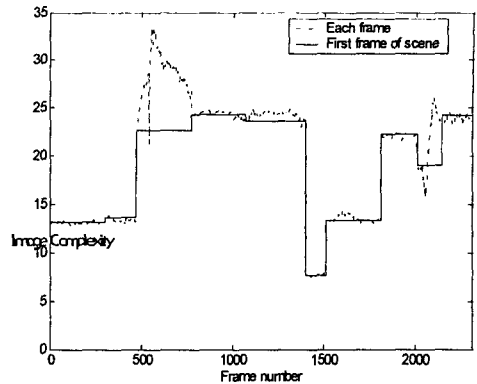


그림 5. 영상의 복잡도



그림 6. 원본영상과 워터마크가 삽입된 영상

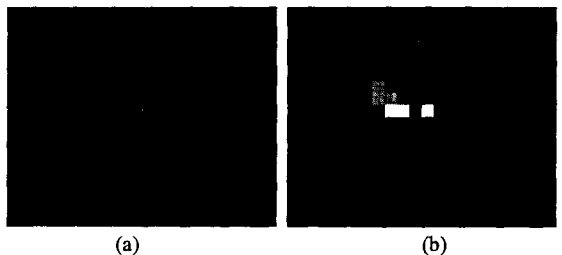


그림 7. (a) 프레임 차이 (b) 움직임 벡터의 크기로 분리된 영역

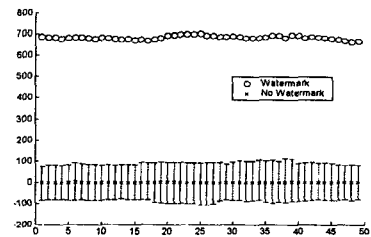
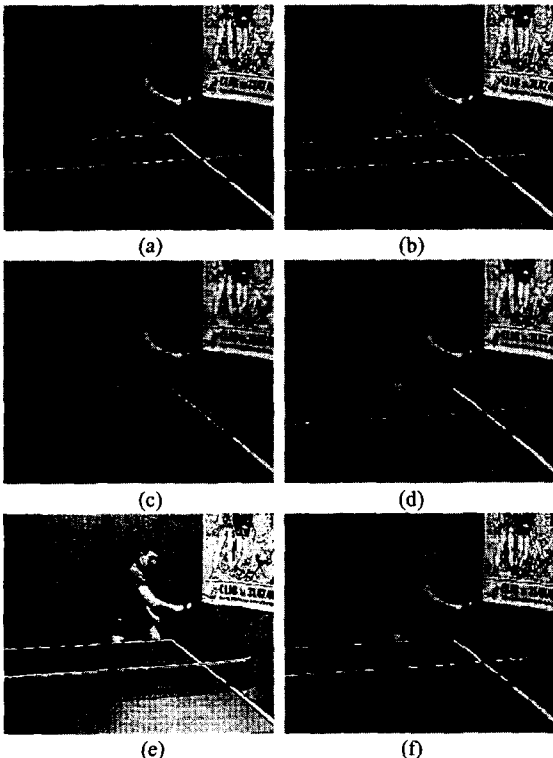


그림 8. 워터마크 검출 결과

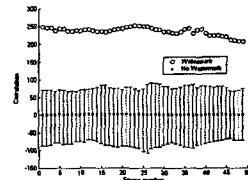
표 1. 워터마크 검출비율

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

워터마크가 삽입된 영상에 다양한 공격을 가하여 제안된 알고리즘의 강인성을 시험하였다. 그림 9는 공격이 가해진 영상이고 그림 10은 각각의 공격을 가한 후 워터마크를 검출한 결과이다. 그림에서 보여지듯이 공격이 가해진 후에도 워터마크가 검출되어 강인성이 보장됨을 알 수 있다.



(a) 원래의 워터마크 삽입 영상, (b) 가우시안 잡음 공격, (c) 저역통과 필터 공격, (d) 중간값 필터 공격, (e) 히스토그램 평활화 공격, (f) 1/2 크기 축소 공격  
그림 9. 워터마크 영상에 대한 다양한 공격 영상



(e) 가우시안 잡음 공격, (b) 저역통과 필터 공격, (c) 중간값 필터 공격, (d) 히스토그램 평활화 공격, (e) 1/2 크기 축소 공격  
그림 10. 다양한 공격에 대한 워터마크 검출결과

### VI. 결론

본 논문에서는 장면단위의 비디오 워터마킹을 이용한 새로운 복사 방지 방식을 제안했다. 먼저, 영상 신호를 장면전환 검출기를 이용하여 의미 있는 장면으로 나누고 이러한 장면들을 단위로 하여 워터마크를 삽입한다. 화면의 복잡도와 움직임 벡터의 크기에 따라 각기 다른 워터마크 삽입강도를 사용한다. 이런 방식을 사용하면 우수한 검출비율과 워터마크의 비가시성을 얻을 수 있다. 장면을 기반으로 한 워터마크가 삽입된 스트림을 이용해 복사 방지 기능이 가능하다. 이러한 방법은 또한 불법복제 추적에 적용될 수 있다. 즉, 콘텐츠의 소유자는 'fingerprint'를 이용하여 불법복제를 시작한 사용자를 추적할 수 있다. 이 경우 사용자의 고유번호를 워터마크 형태로 삽입함으로써 누가 최초로 저작권 침해행위를 범했는지 판별하게 된다.

### 참고문헌

- [1] 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, Feb. 2002.
- [2] T. Kalker, "System issues in digital image and video watermarking for copy protection," *IEEE International Conference on Multimedia Computing and Systems*, Vol. 1, pp. 562-567, 1999.
- [3] 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.
- [4] 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.
- [5] Y. K. Seong, T. S. Choi, "Scene-based Copy Protection Scheme For Hard Disk Drive Embedded Digital Satellite Receiver," *IEEE International Symposium on Consumer Electronics*, pp. D7-D10, Germany, Sep. 24-26, 2002