

# H.264/AVC와 SVC를 위한 Fragile watermarking 기반의 효율적인 인증 기법

박수완\*, 신상욱\*

\* 부경대학교 정보보호 협동과정

e-mail : music016@pknu.ac.kr, shinsu@pknu.ac.kr

## An Efficient Authentication Scheme based on Fragile Watermarking for H.264/AVC and SVC

Su-Wan Park\*, Sang-Uk Shin\*

\*Dept. of Information Security Graduate School, Pukyong National University

### 요 약

본 논문은 비디오 압축 기술인 H.264/AVC와 H.264/SVC에 적용할 수 있는 인증 목적의 효율적인 프래자일(fragile) 워터마킹 기법을 제안한다. 제안된 워터마킹 기법은 H.264/AVC 비디오 부호화기에서 압축률을 높이기 위해 사용하는 매크로블록(MB) 예측 모드들을 특징 값으로 추출하여 콘텐츠 제공자의 비밀키로 암호화 후 워터마크로 사용하는 인증 기법으로, 이는 공간적, 시간적 그리고 SNR 확장성을 가지는 H.264/SVC에도 확장하여 적용할 수 있다. 워터마크 삽입은 최적의 예측 모드를 찾기 위한 모드 결정과정에서 수행되어 워터마크 후에도 최적화 된 콘텐츠를 얻을 수 있으며, 간단한 연산을 엔코더와 결합시켜 낮은 시간 증가율을 가진다.

### 1. 서론

최근 컴퓨터 기술과 인터넷 기술의 발달과 함께 이미지, 비디오 그리고 오디오와 같은 디지털 콘텐츠의 사용이 급증하고 있다. 특히 위성이나 케이블, 인터넷 망과 같은 공개적인 경로를 통해 유포되는 사적인 디지털 비디오의 경우, 사용자가 생성자의 허가 없이 콘텐츠를 복사하거나 불법적으로 수정할 수 있어 이를 위한 보호 기술의 필요성은 더욱 강조되고 있다.

불법적인 수정과 저작권자의 권한을 보호하기 위한 해결방안 중 하나는 디지털 비디오 인증 기법으로 크게 3가지로 나눌 수 있다.

첫 번째, 디지털 서명 기반 비디오 인증(digital signature-based video authentication)은 전통적인 암호화적 서명 스킴을 직접적으로 사용하는 방법으로, 비디오 데이터의 해쉬 값을 서명해서 전송하는 방법이다.

두 번째, 미디어 기반 비디오 인증(media signature-base video authentication)은 비디오 콘텐츠 내에 비디오 데이터로부터 추출된 특징이나 특징의 해쉬 값을 사용하는 방법이다. 앞에 두 방법은 콘텐츠와 인증을 위한 서명 값이 분리되어 전송되는 한계를 가진다.

세 번째, 워터마킹 기반 비디오 인증(watermarking-based video authentication) [3-8]은 인증을 위한 워터마크를 오리지널 비디오 데이터 내에 삽입하는 기법이다.

따라서 제안 기법은 현재 비디오 압축 기술로서 높은 효율성과 다양한 확장성을 가지는 H.264/AVC [1]와 H.264/SVC [2] 부호화 안에서의 인증을 효율적으로 수행하기 위해, 미디어 기반 비디오 인증 기법과 같이 비디오 데이터로부터 특징을 추출하고 암호화 한 뒤 추출된 특징 값을 워터마크로 삽입하는 워터마킹 기반 비디오 인증 기법을 사용한다.

### 2. 제안 기법

제안 기법은 비디오 콘텐츠의 무결성을 보장하기 위한 인증 기법 중 하나로 H.264/AVC 비디오 부호화 과정 안에서 효율적인 압축을 위해 사용되어지는 매크로블록(MB)을 위한 예측 모드들을 특징 값으로 사용하여 워터마크하는 미디어 서명 기반 비디오 인증 기법이다.

H.264/AVC는 전후 프레임과 상관없이 독립적으로 압축을 수행하는 I-프레임과 움직임 예측/보상(Motion Estimation/Compensation) 과정을 거쳐야 하는 P와 B-프레임으로 구성된다. 그 중, I-프레임의 휘도 블록은 16×16 블록 단위를 위한 4가지 예측 방향과 4×4 블록 단위를 위한 9가지 예측 방향을 가지는 인트라(Intra) 예측 모드로 각 MB를 부호화하고, P와 B-프레임은 SKIP, 6×16, 16×8, 8×16, P8×8블록 단위로 움직임 예측을 통해 부호화되는 인터(Inter) 모드를 사용하며 P8×8 모드는 다시 각각의 8×8 블록으로 예측되는 서브블록(Sub\_block) 안에서 8×8, 8×4, 4×8, 4×4 중의 하나로 나누어질 수 있다. 이 값들은 다음의

(표1)과 같이 Block\_modes, Intra prediction Modes 그리고 Sub\_block prediction Modes를 통해 표시된 후 비트스트림으로 표현된다.

(표1) 인트라와 인터 예측 모드들의 값 표현

	Block Modes	MB prediction mode values	Sub_block prediction mode value	
Intra Modes	16×16	0 (mode 0)		
		1 (mode 1)		
		2 (mode 2)		
		3 (mode 3)		
	4×4	6	0 (mode 0)	
			1 (mode 1)	
			2 (mode 2)	
			3 (mode 3)	
			4 (mode 4)	
			5 (mode 5)	
Inter Modes	SKIP	0		
	16×16	1		
	16×8	2		
	8×16	3		
	8×8	4	8	
	8×4		9	
	4×8		10	
4×4	11			

먼저, 워터마크로 사용될 인트라와 인터 예측 모드들의 특징값 추출 방법에 대해서 설명한다. I-프레임의 MB은 휘도 성분을 위한 16×16의 4가지와 4×4 블록의 9가지 인트라 예측 모드 중 비트율-왜곡 비용이 최소화 되는 모드를 최종 매크로 블록 모드로 결정한다. 움직임 예측을 위한 P와 B-프레임의 인터 모드는 SKIP, 16×16, 16×8, 8×16, P8×8 블록 단위의 예측 모드 중 최적의 모드를 선택하고, P8×8이 선택될 경우는 다시 8×8, 8×4, 4×8, 4×4 중의 최적의 모드를 각 8×8 서브블록을 위한 모드로 선택하게 된다. 이 때, Intra의 16×16과 Inter의 SKIP, 16×16, 16×8, 8×16를 표현하는 MB\_modes는 각 MB을 위한 특징 값으로 사용하고, Intra의 4×4를 위한 Intra Prediction Modes와 Inter의 P8×8을 표현하는 Sub\_Mb Modes은 각 4×4와 8×8 블록을 위한 특징 값으로 사용된다. 이들 특징 값들은 안전성을 높이기 위해 콘텐츠 제작자 또는 공급자의 비밀키로 암호화(E())하고, 삽입량을 조절하기 위해 식(1)과 같이 p로 나눈 나머지 값을 워터마크(W)로 사용한다.

$$W = E(F) \text{ mod } 2^p \quad (1)$$

다음은 워터마크 삽입 기법이다. 앞에서 얻어진 각 MB 또는 서브블록을 위한 워터마크는 자신의 블록 안에서 예측 모드에 의해 차분된 값들을 DCT와 양자화 한 후 얻어진 계수 값에 삽입한다. 이 때, 각 MB을 위한 워터마크 값은 다음 식(2)와 같이 2진수로 표현한다.

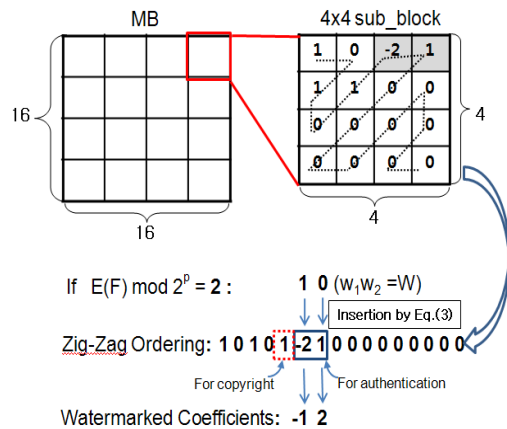
$$W = w_0 w_1 \dots w_{p-1} \quad (2)$$

그리고 워터마크 W를 구성하는 각 비트( $w_i$ )는 양자화 된 0이 아닌 계수( $c_o$ )들의 개수가 p개 이상 존재하는 블록에 한해서 삽입되고, 삽입 방법은 zig-zag ordering의 마지막 p개의 픽셀에 워터마크 비트를 다음의 식(3)과 같이 삽입한다.

$$\text{if } w_i = 0, \quad c_o' = \begin{cases} c_o + 1, & f(c_o > 0 \text{ and } (|c_o| \text{ mod } 2 = 1), \\ c_o - 1, & f(c_o < 0 \text{ and } (|c_o| \text{ mod } 2 = 1), \\ c_o, & \text{otherwise,} \end{cases} \quad (3)$$

$$\text{if } w_i = 1, \quad c_o' = \begin{cases} c_o - 1, & \text{if } (c_o > 0 \text{ and } (|c_o| \text{ mod } 2 = 0), \\ c_o + 1, & \text{if } (c_o < 0 \text{ and } (|c_o| \text{ mod } 2 = 0), \\ c_o, & \text{otherwise,} \end{cases}$$

예를 들어 p가 2이고 암호화 된 워터마크를 2로 가정할 때, 워터마크 과정과 결과는 (그림 1)와 같다.



(그림 1) 제안된 인증 워터마크 삽입 방법

정리하면, MB\_mode를 특징 값으로 사용한 워터마크는 16개의 4×4 블록에 반복적으로 삽입되고, Intra Prediction Mode를 사용한 워터마크는 하나의 4×4블록을 위해 사용되며, Inter의 Sub\_block Mode는 4개의 4×4에 반복적으로 삽입될 수 있다. MB 또는 서브블록이 SKIP되거나 각 4×4블록 내에 0이 아닌 계수의 개수가 p개 이하일 경우에 워터마크는 삽입되지 않지만, 영상에 손상이 생기면 다르게 부호화 된 계수 값에 의해 손상 여부를 확인할 수 있으므로 인증은 이루어진다.

그리고 제안 기법은 MB의 예측 모드 결정 단계에서 워터마크를 삽입한 후, 최적의 예측 모드를 결정함으로써 비트율-왜곡에 의한 손실을 최소화한다.

다음은 수신 측의 워터마크 된 비디오의 검증단계를 설명한다. 수신된 비디오의 각 프레임은 부호화와 마찬가지로 MB 단위로 처리된다. 각 MB은 16개의 4×4블록으로 다시 나뉘고, 각 블록에 0이 아닌 계수 값이 p개 이상 존재한다면, zig-zag

정렬의 마지막 p개의 픽셀로부터 식(4)과 같이 워터마크를 구성하는 비트들을 추출한다. 그리고, 식(5)와 같이 계산하여 워터마크 값을 생성한다.

$$w_i = (|c_i| \bmod 2) \quad (4)$$

$$W = w_0 \times 2^{p-1} + w_1 \times 2^{p-2} + \dots + w_{p-1} \times 2^0 \quad (5)$$

이후, 얻어진 워터마크(W)는 식(6)과 같이 해당하는 MB의 헤더에 포함된 MB\_mode, Intra Prediction Mode 또는 Sub\_block Mode와 비교되고, 일치하면 무결성을 검증하게 된다.

$$\text{if } D(W) = (PM \bmod 2^p), \text{ MB is authenticated,} \quad (6)$$

$$\text{else MB is not authenticated,}$$

다음은 제안 기법을 H.264/SVC로 확장하여 적용하는 방법에 대해 설명한다. H.264/SVC는 H.264/AVC를 기반으로 하는 기본계층(Base Layer)과 공간적, 시간적 그리고 SNR 확장성을 가지는 강화계층(Enhancement Layer)으로 나뉜다. 기본계층은 앞에서 언급한 바와 같이 적용되고, 강화계층에 해당하는 프레임들은 그 특성을 다시 고려해야 한다. 공간적 그리고 SNR 확장성을 가지는 프레임들은 대부분 기본계층을 통해 차분값들(residual data)만 처리하므로, 그것을 나타내는 MB 모드를 특징 값으로 사용하면 앞에서 서술한 방법을 그대로 적용할 수 있다. 그리고, 시간적 확장성을 가지는 프레임은 기본계층에서 설명한 움직임 예측 모드를 그대로 적용하면 된다. 따라서 제안된 기법은 H.264/AVC 뿐 아니라 H.264/SVC에서도 효율적으로 적용할 수 있다.

### 3. 실험결과

우리는 제안 기법을 MPEG SVC 시퀀스들을 가지고 JSVM 9.8에서 실험하였다. 실험은 각 QCIF@7.5HZ와 CIF@15HZ 를 가지는 'football' 과 'foreman' 을 가지고 수행하였으며, 총 프레임수는 100프레임, GOPSize는 8 그리고 Intra\_Period는 16으로 설정하였다.

제안된 기법이 적용된 콘텐츠는 (표2)에서와 같이 화질 저하가 거의 없었으며 낮은 계산복잡도로 인해 수행시간 증가율도 낮아 실시간 응용에 적용 가능하다. 하지만 (표3)에 보여지는 것과 같이 bit-rate 증가율이 다소 높게 나타나지만, 이것은 향상된 시스템 성능과 엔코더 기능에 의해 보완될 수 있다.

(표2) 제안기법이 적용된 비디오들의 PSNR

Condition	Video size	Football			Foreman		
		Y	U	V	Y	U	V
Original (Encoded) video	QCIF	35.25	39.01	40.67	36.86	41.14	42.32
	CIF	34.53	39.44	41.15	35.93	40.80	43.03
Watermarked video for Auth.	QCIF	34.93	39.03	40.65	36.59	41.12	42.35
	CIF	34.49	39.44	41.12	35.86	40.78	43.06

(표3) 워터마크 된 비디오들의 bit-rate 증가율

Video sequence	Football		Foreman	
	QCIF	CIF	QCIF	CIF
Watermarked video for Auth.	4.78%	2.54%	6.02%	3.09%

### 4. 결론

제안된 기법은 H.264/AVC와 H.264/SVC에 적용할 수 있는 프레자일 워터마킹 기반의 효율적인 인증 기법이다. H.264/AVC 엔코더에서 압축 효율성을 높이기 위해 제안된 예측 기법을 통해 결정된 각 블록의 예측모드들은 콘텐츠 제공자의 비밀키로 암호화되어 워터마크로서 사용된다. 콘텐츠에서 추출된 워터마크는 예측 후 남은 잔여 데이터의 DCT와 양자화 과정 후 삽입되며, 같은 방법으로 공간적, 시간적 그리고 SNR 확장성을 가지는 H.264/SVC에도 확장하여 적용할 수 있다. 워터마크 삽입은 최적의 예측 모드를 찾기 위한 모드 결정과정에서 수행되어 워터마크 후에도 최적화 된 콘텐츠를 얻을 수 있으며, 계산 복잡도가 낮고, 엔코더와 결합되어 시간 증가율 또한 매우 낮다.

### Acknowledgement

본 연구는 교육과학기술부와 한국산업기술재단의 지역혁신인력양성사업과 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업[2007-S019-03, 정보투명성 보장형 디지털 포렌식 시스템 개발]의 일환으로 수행된 연구결과임.

### 참고문헌

- [1] "Draft ITU-T recommendation and final draft international standard of joint video specification (ITU-T Rec. H.264/ISO/IEC14496-10 AVC)", in Joint Video Team(JVT) of ISO/IEC MPEG and ITU-T VCEG, JVTG050, 2003.
- [2] ISO/IEC JTC 1/SC 29/WG 11 N8750: Joint Scalable Video Model (JSVM), Marrakech, Morocco, January 2007.
- [3] S. M. Kim, S. B. Kim, Y. Hong, and C. S. Won, "Data Hiding on H.264/AVC Compressed Video", ICIAR 2007, LNCS 4633, pp. 698-707, 2007
- [4] D. Pröfrock, H. Richter, "H.264/AVC video authentication using skipped macroblocks for an erasable watermark," proceedings of SPIE, v. 5960, no. 3, 2005, pp. 1480-1489.
- [5] M. Noorkami and R. M. Mersereau, "Compressed-domain Video Watermarking for H.264", IEEE International Conference on Image Processing, Sep. 2005, vol. 2, pp. 11-14, 2005
- [6] J. Zhang and A. T. S. Ho, "Efficient Video Authentication for H.264/AVC," ICICIC06, vol. 3, Aug. 2006, pp. 46-49.
- [7] B. G. Mobasserri and Y. N. Raikar, "Authentication of H.264 streams by direct watermarking of CAVLC blocks," proceedings of SPIE, v. 6505, 2007, pp.65051-65055.
- [8] T. Y. Chen, T. H. Chen, Y. T. Lin, Y. C. Chang and D. J. Wang, "H.264 Video Authentication Based on Semi-fragile Watermarking," IHHMSP 08, Aug. 2008, pp. 659-662.