블록계층의 DC/AC 성분을 이용한 인증과 서명의 이중 비디오 워터마킹에 관한 연구

부희형, 박성미, 배호영, 이배호
전남대학교 컴퓨터정보통신공학과
e-mail: bhh0106@hanmail.net

A Study on the Dual Video Watermarking for Authentication and Signature using DC/AC Components of Block Layer

Hee-Hyung Boo, Seong-Mi Park, Ho-Young Bae, Bae-Ho Lee
Dept. of Computer Engineering, Chonnam National University

요 약

본 논문에서는 디지털 비디오 인코딩 과정의 VLC(variable length coding) 영역에서 블록계층의 DC/AC 성분을 이용한 인증과 서명의 이중 비디오 워터마킹 시스템을 제안하였다. 제안한 기법은 블록계층의 DC 성분과 AC 성분에서 HVS(human visual system)의 특성을 고려한 것이다. 인증 워터마킹은 주요한 정보를 포함하는 저주파 영역과 윤곽선 정보를 포함하는 중간 주파수 영역을 이용하여 인트라 프레임의 DC 성분과 움직임 벡터의 부호를 변형시켰고, 서명 워터마킹은 모든 프레임의 AC 성분들 중에서 마지막 AC 성분의 Level이 '1'인 경우에만 워터마크를 삽입하였다. 서명 워터마크 검출은 저작권자의 비밀 키에 의해서만 가능하고, 기술적인 면에서 저작권자의 판별 기준이 될 수 있다. 제안한 이중 비디오 워터마킹 시스템의 특징은 인증과 서명의 두 가지 기능을 선택적으로 수행할 수 있으며, 계산과정이 복잡하지 않으면서 비트 스트림(bit-stream)을 유지시킨다. 그리고 실험 결과에서 기존의 방법보다 화질 면에서 2~3dB 더 높은 수치를 얻어 우수함을 보였고, 인코딩 수행 속도에 미치는 영향은 거의 없었으며, 향후 실시간 인코딩 처리에 응용될 수 있다..

1. 서론

최근 인터넷과 디지털 멀티미디어 기술의 발전은 네트워크와 저작 툴의 발전을 가져왔고, 디지털 콘텐츠를 개인이 직접 저작 및 배포하는 개인방송 기술과 P2P 공유 기술의 형태는 디지털 콘텐츠의 배포 및 유통을 더욱 빠르게 진행시키고 있다. 이에 따라 디지털 콘텐츠의 저작 권리와 지적 재산권의 보호, 무단 복제 및 배급에 대한 차단이 요구되어 DRM(digital right management) 기술에 대한 개발의 요구가 강력히 대두되었다[1]. 특히, 디지털 비디오 워터마킹 기술은 비디오 스트림에서 DRM 기능의 최적의 방법이라 할 수 있다.

기존의 비디오 워터마킹 기법은 크게 압축 도메인과 비 압축 도메인의 삽입구조로 나눌 수 있다. 압축 도메인의 비디오 워터마킹은 DCT 계수, 모션 벡터, GOP 구조 등의 정보를 이용하는 방법들이 있다[1,2,3,4]. 대표적인 예로 Langelaar[2,5]는 AC 성분에서 lc-VLC(label-bit-carrying VLC)와 pc-VLC(pattern-carrying-VLCs) 조건을 이용하여 코드워드의 길이가 증가되지 않는 범위 내에서 정보를 삽입하는 방법을 제안하였다. 그 방법은 적용이 쉽고, re-encoding에도 강한 장점이 있다. 하지만 워터마크의 값과 AC의 값에 의존적이고, 중간 주파수 영역의 사용으로 화질 저하의 우려가 있다. 제안한 이중 비디

오 워터마킹 기법은 HVS(human visual system)의 특성을 고려한 방법으로 인증 워터마킹은 주요한 정보를 포함하고 있는 저주파 영역과 윤곽선 정보를 포함하고 있는 중간 주파수 영역에 민감한 반응을 보이는 HVS[6,7]의 특성에 착안하여 인트라 프레임의 DC 성분과 움직임 벡터의 부호를 변형시켰다. 그리고 서명 워터마킹은 고주파 영역에 둔감한 반응을 보이는 HVS의 특성에 착안하여 AC 성분들 중에서 마지막 AC의 Level이 '1'인 경우에만 저작권자의 정보를 삽입하였다.

2. RSA 공개 키 암호화와 M 시퀀스

이중 비디오 워터마킹 시스템의 인증 워터마크는 두 신호 사이에 상호연관이 없어야 한다는 특성을 가진 M 시퀀스에 의해 생성된 127 비트열(bit-stream)을 사용하였고, 서명 워터마크는 RSA(Rivest-Shamir-Adelman) 공개 키 암호화를 적용하여 이진 변환 후, '0'은 '1'로, '1'은 '-1'로 치환하여 사용함으로써 워터마크의 신뢰도를 높였다. 다음은 워터마크의 정보를 생성하기 위한 RSA 공개 키 암호화 기법과 M 시퀀스를 설명하였다.

(1) RSA 공개 키 암호화

소인수 분해의 어려움에 안전도의 근간을 두고 있는 RSA 암호화 기법은 n 비트의 길이를 갖는 메시지 블록, 공개 키(public key), 비밀 키(private key), 그리고 모듈러스(modulus) 수를 사용하여 암호화, 복호화 연산을 수행한다. RSA 알고리즘의 공개 키와 비밀 키를 계산하기 위한 절차는 아래와 같다.

① 큰 수인 두 개의 소수 p, q를 정한다.

② $n = p \times q$를 계산한다.

③ $\phi(n)$를 다음과 같이 정의한다.

- $\phi(n) = (p-1) \times (q-1)$로 정의하고 계산한다.

④ $\gcd(e, \phi(n)) = 1$을 만족하는 e 값을 결정한다. 여기서, e와 $\phi(n)$는 서로 소이고, $e<\phi(n)$을 만족해야 한다.

⑤ $ed \equiv 1 \pmod{\phi(n)}$를 만족하는 d를 정한다. 여기서, $d < \phi(n)$이다.

평문 m을 암호화하기 위해서는 두 개의 양의 정수로 구성된 공개 키 (e, n)를 이용하여 m^e를 계산한 후, n으로 나눈 나머지를 암호문 C로 만든다. 역으로, 복호화는 비밀 키 (d, n)를 이용하여 암호문 C를 d번 곱한 후, n으로 나누게 되면 나머지가 원래의 평문 m이 된다.

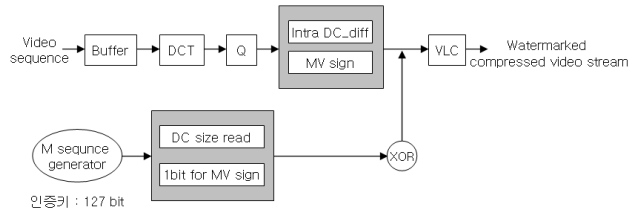
(2) M 시퀀스

인증 워터마크의 정보는 천이 레지스터(feedback shift register)에 의해 생성되는 M 시퀀스를 사용하였다. 실험을 위해 7 비트 레지스터에서 127 비트열(bit-stream)을 주기적으로 생성하여 인증 키로 사용하였다.

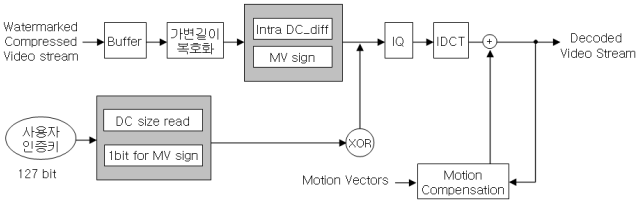
3. 블록계층의 DC/AC 성분을 이용한 이중 비디오 워터마킹

제안된 시스템의 워터마킹 기법은 HVS의 특성 중에 핵심 부분만을 사용하여 계산 시간을 줄였다. HVS는 주요 정보를 포함하는 저주파 영역과 윤곽선 정보를 포함하는 중간주파수 영역에 민감하고, 상대적으로 고주파 영역에 둔감한 특성을 보인다. 양자화된 8×8 블록에서 DC 계수는 영상의 평균밝기에 해당되고, DPCM 방식으로 부호화되며, AC 계수는 고주파 영역에서 '0'이 많이 나오는 특징이 있고, zig-zag 스캔에 의해 부호화된다.

제안된 시스템에서 인증 워터마킹 기법은 인트라 프레임의 DC 계수의 차이 값과 움직임 벡터의 부호를 인증 키와 XOR 연산을 수행하였다. 인증 키 삽입을 위한 워터마킹 구조는 아래 (그림 1)과 같고, 복호화 과정은 아래 (그림 2)에서 나타내었다.



(그림 1) 인증 워터마킹 블록도



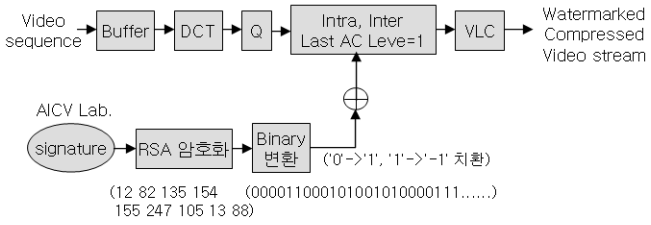
(그림 2) 인증 워터마킹 복호화 블록도

서명 워터마킹 기법은 고주파 영역에 있는 AC 성분들 중에서 마지막 AC 성분의 Level이 '1'인 경

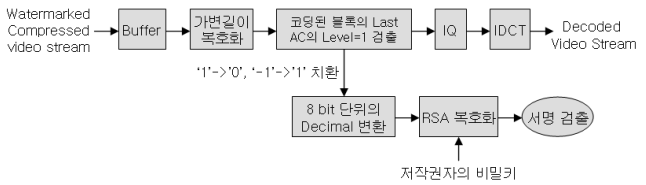
우에만 RSA 암호화된 서명 정보를 삽입하였다. 이 기법은 최대 고주파 영역인 마지막 AC 성분에서 Level 값이 '1'과 '-1'인 경우에만 변형 시키므로 최대 차이 값은 2이며, 그것은 아주 극소한 변화에 해당된다. 즉, 코드워드의 증가를 방지하고, 블록화 현상 등의 문제점들을 해결해주는 이점이 있다. 수행 후, 비트 스트림(bit-stream)은 워터마킹 이전의 비트 스트림과 동일한 길이로 생성되었고, 인코딩 수행 속도의 차이도 거의 보이지 않았다.

서명 워터마크의 검출은 코딩된 블록의 마지막 AC의 Level이 '1'인 경우에만 부호와 함께 추출하여 '1'은 '0'으로, '-1'은 '1'로 치환한 후, 8 비트 단위로 십진 변환하여 RSA 복호화 하면 서명 정보를 검출할 수 있다. 이 기법은 블라인드 워터마킹 기법으로 저작권자의 키에 의해서만 확인이 가능하도록 하였다.

아래 (그림 3)에서 서명 워터마킹 블록도를 나타내었고, 아래 (그림 4)에서 서명 워터마크 검출 블록도를 나타내었다.



(그림 3) 서명 워터마킹 블록도



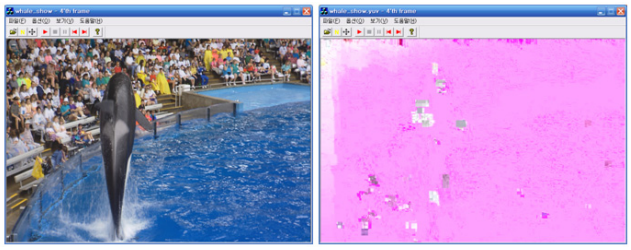
(그림 4) 서명 워터마크 검출 블록도

DRM 기능에서 인증과 서명의 선택적 적용을 위한 환경설정은 아래 <표 1>과 같다.

<표 1> DRM 환경설정

encoder configure	
⋮	
3	{ drm 0: non, 1: authentication, 2: signature, 3: all }
../drm/sig.key	{ signature filename }
../drm/id.key	{ authentication filename }

아래 (그림 5)는 "Whale_Show"의 원 영상과 신호를 변형시킨 영상으로 ⓑ는 적법한 사용자가 아닐 경우의 영상을 나타내었다.



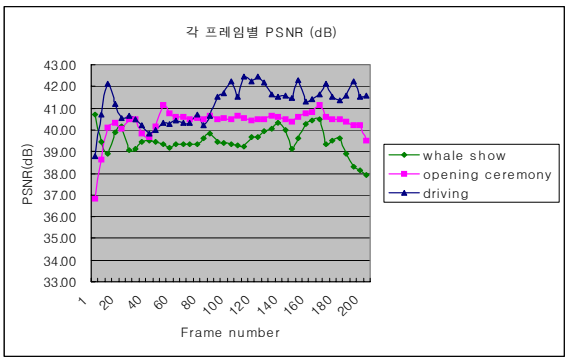
(그림 5) ⓐ 원 영상 ⓑ 인증 워터마킹 후 영상

4. 실험방법 및 결과

제안한 이중 비디오 워터마킹 기법의 실험은 Intel(R) Pentium(R) 4 CPU 3.00GHz, 1.00GB RAM의 윈도우즈 XP 환경에서 Visual C++ 6.0을 사용하여 MPEG-4 FGS 인코더에 DRM 기능을 적용하였다. 실험을 위한 동영상은 SIF(352×288)의 "Flower-Garden", "Table-Tennis", "Mobile" 30frame/s 동영상과 해상도가 높은 SD급(720×480)의 "Whale_Show", "Opening_Ceremony", "Driving" 30frame/s 동영상을 사용하였다. 실험 후, 서명 워터마킹은 객관적 화질 평가인 PSNR(peak signal to noise ratio)을 사용하여 평가 하였고, 인증 워터마킹은 각 동영상의 휘도 성분에 대하여 주관적 화질 평가로 사용되는 weber의 JND(just noticeable difference) 식을 사용하였다.

$$\frac{\Delta I}{I} = k \qquad (1)$$

여기서, ΔI 는 차이 경계치(또는 JND)를 나타내고, I 는 초기 휘도성분의 강도로 나타낸다. 적용결과 약 4-JND의 수치를 얻어 차이가 많음을 알 수 있었다.



(그림 6) 각 프레임별 PSNR (4M bit-rate)

화질 평가에 사용된 PSNR은 peak signal power와 noise power 비율의 log 표현 방법으로 PSNR이 클수록 원 영상에 근접함을 나타낸다. 오차 계산은 MSE(mean squared error) 방법을 사용하였으며, 수식은 아래 식 (2)와 식 (3)과 같다.

$$PSNR[dB] = 10log_{10}\frac{255^2}{MSE}\ [dB] \qquad (2)$$

$$MSE = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(x(i,j)-x'(i,j))^2 \qquad (3)$$

여기서, M과 N은 가로 픽셀과 세로 픽셀 수를 나타내고, $x(i,j)$는 원 영상의 픽셀 값이며, $x'(i,j)$는 서명 워터마크가 삽입된 픽셀 값이다. 위 (그림 6)은 SD급 실험 영상의 프레임별 PSNR의 결과이고, 원 영상과의 화질 차이가 거의 없음을 보였다.

<표 2> 시간대별 프레임들의 평균 PSNR(dB)

동영상	tennis		flower		mobile	
기법 / 시간대	Langelaa(%)	제안(%)	Langelaa(%)	제안(%)	Langelaa(%)	제안(%)
1	43.7	46.1	36.1	38.9	35.1	37.4
2	47.1	49.3	36.3	39.2	35.8	38.7
3	46.6	48.7	36.8	39.7	35.8	38.7
4	46.6	48.7	36.4	39.2	34.8	37.1
5	50.0	52.1	35.3	38.2	35.6	38.4
6	49.5	51.6	36.1	38.9	36.9	39.8

위 <표 2>는 본 논문에서 제안한 서명 워터마킹 기법과 Langelaar의 기법을 비교하기 위한 표이고, 대체적으로 제안한 방식이 2~3dB 더 높은 수치를 얻었다.

5. 결론 및 향후 연구방향

본 논문에서는 RSA 암호화된 저작권 정보와 M 시퀀스를 워터마크로 사용하여 MPEG-4 FGS 인코더에 DRM 기능을 적용하였다. 인증 워터마킹 기법은 HVS에 민감한 영역을 사용하였고, 서명 워터마킹 기법은 HVS에 둔감한 영역을 사용하여 코드워드를 증가시키지 않으면서 효과적으로 수행하는 방법을 보였다. 실험 결과, 서명 워터마킹은 기존의 방법보다 2~3dB 더 높은 수치를 얻어 우수함을 보였고, 원 영상과의 화질 차이는 거의 없었다. 그리고 불법적인 사용을 막기 위한 인증 워터마킹 기법은 저 비트율을 유지하면서 적법한 인증 키에 대해서만 정상적인 수행을 하였다. 개선점으로는 각종 정보보호 시스템에서 기능 모듈로 사용이 가능해야 하고, 디코더 부분에서 복사방지 및 추적기능이 추가되어야 한다. 향후 사용자의 요구가 급증하게 될 실시간 스트리밍 서비스에서 실시간 인코딩 처리의 효율을 높이는 방향으로 더욱 많은 연구가 이루어져야 할 것이다.

참고문헌

[1] A. M. Alattar, E.T. Lin, M. U. Celik, “Digital watermarking of low bit-rate advanced simple profile MPEG-4 compressed video”, IEEE Trans. Circuits Syst. Video Tech. 13 (8) (2003) 787-800.

[2] G. C. Langelaar, R. L. Lagendijk, J. Biemond, “Real-time labeling of MPEG-2 compressed video”, J. Visual Commun. Image Represent. 9 (4) (1998) 256-270.

[3] F. Hartung, B. Girod, “Watermarking of uncompressed and compressed video”, Signal Process. 66 (3) (1998) 283-302.

[4] F. Hartung and B. Girod, “Digital watermarking of MPEG-2 coded video in the bitstream domain”, in Proc. Int. Conf. Acoustics, Speech, Signal Processing ′97, vol. 4, Munich, Germany, 1997, pp.2621-2624.

[5] G. C. Langelaar, R. L. Lagendijk, “Optimal differential energy watermarking of DCT encoded images and videos”, IEEE Trans. Image Process. 10 (1) (2001) 148-158.

[6] J.-F. Delaigle, C. De Vleeschouwer, and B. Macq, “A psycho-visual approach for digital picture watermarking,″ J. Electronic Imaging, vol. 7, no. 3, pp.628-640, July 1998.

[7] T. A. Wilson, S. K. Rogers, and L. R. Myers, “Perceptual based hyperspectral image fusion using multiresolution analysis,″ Opt. Eng., vol, 34, no. 11, pp. 3154-3164, Nov. 1995.