DRM 기반의 디지털 비디오 콘텐츠 보호

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

Digital Video Contents Protection based on DRM

Hee-Hyung Boo, Wu-Ju Lee, Ho-Young Bae, Bae-Ho Lee
Dept. of Computer Engineering, Chonnam National University

요 약

본 논문은 DRM(Digital Rights Management)의 핵심요소기술인 디지털 비디오 워터마킹 기술에서 암호화 기법을 함께 적용하여 저작권 판별 및 콘텐츠 보호의 두 가지 역할을 수행하는 시스템을 제안하고자 한다. 본 논문에서는 저작권 정보를 공개키 기반의 RSA 암호화 방법으로 암호문을 만든 후 이진화 과정을 수행하여 워터마크 키 정보를 생성하였고, 워터마킹 기법으로는 통계적 모델의 계산 속도가 빠른 NVF(Noise Visibility Function) 방식의 Adaptive Stationary GG(Generalized Gaussian) model[1]의 기법을 사용하였다. 암호문은 사용자 컨트롤러에서 제어가 가능하도록 하여 권한이 부여된 사용자만이 재생이 가능하도록 하였다. 본 논문의 구성은 2장에서 암호화 과정을 설명하고, 3장에서는 기존의 기법과는 다른 통계적 접근의 워터마킹 기법을 적용한 과정을 설명하며, 4장에서는 제안한 방법이 실제 환경에서의 실험 결과를 보여준다. 마지막으로 5장에서는 결론과 개선점을 바탕으로 향후 연구방향을 제시한다.

본 논문에서 제안한 방법은 미래사회 인터넷에서의 올바른 디지털 콘텐츠 사용 문화 정책에 큰 역할을 할 것으로 기대된다.

1. 서론

최근 디지털 미디어의 압축 및 전송 기술이 빠르게 발전함에 따라 멀티미디어에 대한 일반 사용자의 관심과 요구가 급격히 증가하게 되었다. 특히, 디지털 영상을 제작하는 각종 도구들이 발달하면서 영상 데이터의 생성, 편집, 저장 등이 쉬워지고 영상을 왜곡 없이 전송하기 위해 장애에 강한 디지털 데이터로의 변경이 확산되고 있다. 이러한 다양한 멀티미디어 저작물들은 개인용 PC 및 가정용 통신 인프라의 급속한 확산과 맞물려 빠르게 유통되고 있으며, 이에 따라 디지털 멀티미디어의 저작 권리나 지적 재산권을 보호하고 무단 복제나 배급을 차단할 기술에 대한 개발 요구가 강력히 대두되었다.

이러한 기술은 최근에도 매우 활발히 연구되어지고 있는 분야로, 디지털 콘텐츠 보호를 위한 암호화 기법(Encryption method)[2]과 저작권 인증과 관련된 디지털 워터마킹 기법(Digital Watermarking method)[3,4,5]이 연구되고 있으며, 콘텐츠 보호 기술의 핵심을 포괄하고 있다.

본 논문에서 다루는 디지털 워터마킹 기술의 응용에 따른 요구사항으로는 비인식성, 중복성, 키 등이 있다. 여기서, 비인식성은 삽입된 정보가 일정 인식 수준 이하로 처리되어야 함을 나타내며, 중복성은 디지털 워터마크가 삽입된 원본의 일부분만으로도 복원이 가능하도록 고려되는 사항이다. 키는 사용자의 조작이나 삽입된 정보의 삭제 등을 목적으로 하는 악의적인 공격으로부터 삽입된 워터마크를 보존하려는 수단으로 사용된다. 이와 같은 고려사항들은 강하게 혹은 약하게 반영함으로써 다양한 디지털 워터마킹 응용들을 생성할 수 있는데, 현재까지 부각된 대표적인 워터마킹 응용들로는 저작권 보호,

복사 방지, 인증, 보급 추적 등이 있다.

본 논문에서는 기존의 DCT, FDCT, DFT, DWT 등의 워터마킹 접근 기법[6,7,8]과는 다른 통계적인 기법[1]을 사용하였으며, RSA 암호화 기법과 혼합하여 불법적인 사용자로부터 데이터를 안전하게 보호하고, 저작권 정보를 사용함으로써 소유권을 인증하는 방법을 사용하였다. RAS 공개키 방법으로 생성된 워터마크는 MPEG-4 인코더에 적용하였으며, 향후 MPEG-4 FGS 인코더의 하위계층에 적용을 고려한 방법으로 I-프레임에 적용하였다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 저작권 정보에 대해 공개키 기반의 RSA 비대칭 암호화 기법의 적용을 기술하고, 3장에서는 워터마크 키를 통계적 접근 방법의 NVF(Noise Visibility Function)[1]에 적용시킨 부분에 대해 다루며 4장에서는 실험 및 구현, 그리고 마지막으로 5장에서는 결론 및 향후 연구방향으로 마무리 한다.

2. RSA 공개키 암호화 알고리즘

본 논문에서는 인터넷 스트리밍 서비스에서 발생할 수 있는 디지털 비디오 콘테츠에 대한 저작권 보호 문제와 불법복제의 방지를 위한 방법으로 RSA 공개키 암호시스템을 이용하였다. 이 기법은 소인수분해의 어려움에 안전도의 근간을 두고 있고, n-비트의 길이를 갖는 메시지 블록, 공개키(public key), 비밀키(private key) 그리고 모듈러스(modulus) 수를 사용하여 암호화, 복호화 연산을 한다.

RSA 알고리즘의 공개키와 비밀키를 계산하기 위해서는 아래절차를 수행한다

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 e값을 결정한다. 여기서 e와 $\phi(n)$는 서로 소이고 $e<\phi(n)$을 만족해야 한다.

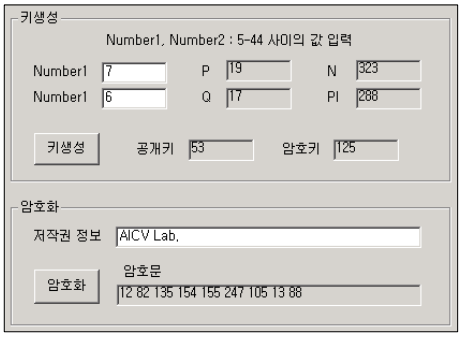
⑤ $ed \equiv 1 \pmod{\phi(n)}$를 만족하는 d를 정한다. 여기서 $d < \phi(n)$이다.

이제 위의 다섯 가지의 절차를 거쳐 RSA 알고리즘에서 공개키로 암호화하는 방법과 복호화하는 방법을 설명하면 다음과 같다.

<표 1> 암호화와 복호화

공개키 : n, e
비밀키 : d
암호화 : $C \equiv m^e \pmod{n}$
복호화 : $m \equiv C^d \pmod{n}$

평문 m을 암호화하기 위해서는 두 개의 양의 정수로 구성된 공개키 (e, n)를 이용하여 m^e를 계산한 후, n으로 나눈 나머지를 암호문 C로 만든다. 역으로 복호화는 비밀키 (d, n)를 이용하여 암호문 C를 d번 곱한 후 n으로 나누게 되면 나머지가 원래의 평문 m이 된다. 아래 그림은 통합 시스템에서의 암호화 과정을 보여준다.



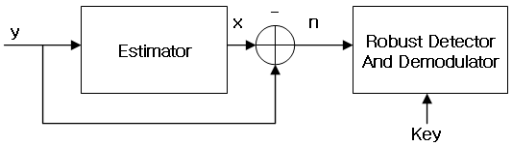
(그림 1) RSA 암호화 키 생성

본 논문에서는 저작권 정보에 AICV Lab.을 넣어 암호화 과정을 수행하였다.

3. 통계적 접근의 워터마킹 기법

2장에서 암호화 시스템에 의해 생성된 암호문은 이진화 과정을 수행하고 인코더의 VLC(Variable Length Coding) 과정 후 적응적으로 삽입한다. 이 과정은 향후 개발 계획인 MPEG-4 FGS 기반의 인코더에 적용을 고려한 것이다. 본 논문에서 사용한 워터마킹 기법은 통계적 모델의 계산 속도가 빠른 NVF(Noise Visibility Function)을 이용한 Adaptive Stationary GG(Generalized Gaussian) model[1]의 기법을 적용하였다. 적용한 기법은 워터마크가 삽입

된 영상과, 잡음을 추정하고, 적응적인 삽입강도를 활용한 방법이다.



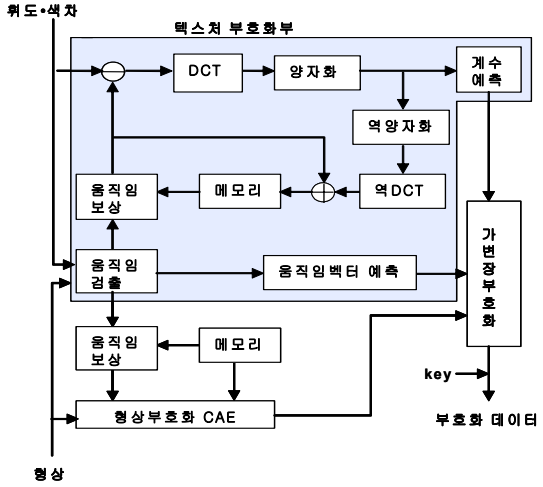
(그림 2) 워터마크 삽입과 검출 블록도

위 (그림 2)의 블록도에서 y는 원영상이고, x는 워터마크가 삽입된 영상이며, n은 워터마크 정보에 해당된다.

여기서 적응적 워터마크의 은닉을 위해 아래 식 (1)과 같은 감마 함수를 이용한다.

$$\Gamma(t) = \int_0^{\infty} e^{-u} u^{t-1} du \qquad (1)$$

아래 (그림 3)은 MPEG-4 동영상 부호화 과정에서 워터마크 키를 삽입하는 구조를 나타낸다.



(그림 3) MPEG-4 인코더 워터마크 삽입 구조

본 논문에서는 4장에서 Adaptive Stationary GG(Generalized Gaussian) model을 이용함으로써 워터마크 삽입 후의 비가시성을 확보할 수 있음을 보인다.

4. 실험 및 결과

본 논문에서 제안한 방법의 실행을 위하여 윈도우즈 XP 환경에서 Visual C++ 6.0을 이용하여 실험하였다. 실험 영상은 모두 CIF 포맷의 프레임 사이즈 352×288 으로 Akiyo, Children2, Stefan을 사용하였다. 실험 후 결과 영상의 화질을 평가하기 위해 프레임별로 PSNR(Peak Signal to Noise Ratio)을 적용시켜 보았다<표 3>.

<표 3> 워터마킹 된 비디오 프레임의 PSNR

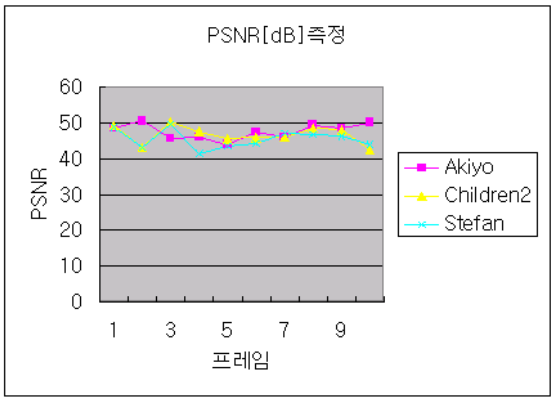
No	Akiyo	Children2	Stefan
1	48.73	49.34	48.79
2	50.63	43.25	43.31
3	45.87	50.46	49.62
4	46.13	47.67	41.63
average	47.84	47.68	45.84

적용된 PSNR(Peak Signal to Noise Ratio)의 식은 아래와 같다.

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

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

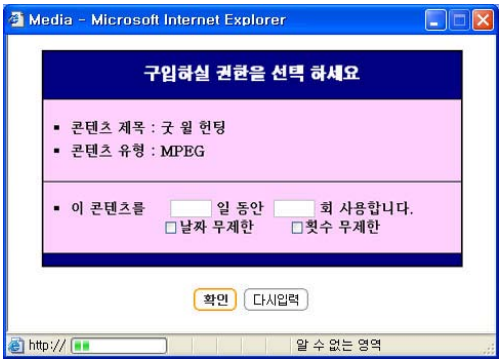
식(3)에서 M과 N은 원 영상의 가로 픽셀과 세로 픽셀 사이즈를 나타내고, $x(i,j)$는 원 영상의 픽셀 값이며 $x'(i,j)$는 워터마크가 삽입된 영상의 픽셀값이다. PSNR 값이 50에 가까울수록 원 영상과 화질의 차이가 적음을 알 수 있었다. 여기서 MSE는 원 영상과 워터마크가 삽입된 영상 간의 평균자승오차(Mean Square Error)이다. PSNR의 분포는 아래 (그림 4)와 같다.



(그림 4) 프레임의 PSNR 분포

아래 (그림 5)는 사용자 플레이어에서 권한 부여

가 안 된 사용자에게 DRM 기능을 적용한 결과화면을 보여준다.



(그림 5) 사용자 권한 확인

사용자 권한확인의 처리과정은 ① 사용자 인증확인 후 ② 워터마크의 존재유무를 판별하고, ③ 워터마크 검출 과정에서 비밀키의 소유 여부를 확인한다. ④ 만약 비밀키를 소유하지 않을 경우 구매요청의 메시지를 보내고, 그렇지 않을 경우 비디오를 재생시키는 과정을 수행한다.

5. 결론 및 향후 연구방향

본 논문에서는 암호화된 저작권 정보를 워터마크로 사용하여 MPEG-4 인코더에 적용하는 방법을 제시하였다. 제안한 방법에서는 인간의 비가시성을 고려하면서 효율적으로 워터마크를 삽입할 수 있는 방법을 보였다. 실험 결과 후, 영상의 화질 비교 결과 원영상과의 화질 차이는 거의 없었으며, 불법적인 사용을 막기 위한 DRM 기능 또한 확실하게 수행됨을 보였다.

개선점으로는 향후 각종 정보보호 시스템의 기능 모듈 또는 시스템으로의 사용을 위해 워터마킹 기술의 독립성이 요구되고, RSA 공개키 암호화 방법의 계산 복잡도 감소가 필요하며, 각 모듈별 하드웨어로의 구현이 필요하다. 마지막으로 향후 인터넷 개인 방송 기술과 관련하여 인코더 부분에서 HDTV급에 대응되는 영상 화질 개선과 Real-Time으로의 실시간 처리효율 등에 더 많은 연구가 이루어져야 할 것이다.

참고문헌

[1] S. Voloshynovskiy, A. Herrigel, N. Baumgaerter, and T. Pun, "A Stochastic Approach to Content Adaptive Digital Image Watermarking," Third Information Hiding Workshop, 1999.

[2] Peter Wayner, Digital Copyright Protection, AP Professional, pp.13-34, 1997.

[3] Rolf Oppliger, Security technologies for the World Wide Web, Artech House, pp.307-320, 1999.

[4] X. Xia, C. G. Boncelet, G. R. Arce, "A Multiresolution Watermark for Digital Images", Proc. IEEE ICIP, Vol.3, pp.548-551, 1997.

[5] D. Kundur, D. Hatzinakos, "A Robust digital image watermarking method using wavelet-based fusion", IEEE ICIP, Santa Barbara, California, Vol.1, pp.544-547, Oct. 1997.

[6] Ingemar J. Cox, Joe Kilian, Tom, Leighton and Talal. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans, on Image processing, Vol.6, No.12, pp.1673-1687, 1997.

[7] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, " A Secure, Robust Watermark for Multimedia", Workshop on Information Hiding, Newton Institute, Univ. of Cambridge, May 1996.

[8] S. Craver. N. Memon, N. Y대, and M. Yeung, "Can Invisible Watermarks Resolve Rightful Ownership?" IBM Research Report, RC 20509, July 25, 1996.