워터마크를 이용한 멀티미디어 컨텐츠의 저작권 보호

Copyright Protection of Multimedia Contents Using Watermark

석종원, 홍진우

Jong Won Seok, Jin Woo Hong

ETRI 방송기술연구부

요약

최근들어 디지털 워터마킹(watermarking) 기법이 디지털 멀티미디어 컨텐츠 저작권 보호를 위한 새로운 해결책으로 제시되고 있으며, 국내외에서 이와 관련된 연구가 활발히 진행되고 있다. 본 논문에서는 문서, 영상, 그리고 오디오등의 멀티미디어 컨텐츠 보호를 위해 사용되는 대표적인 워터마킹 기법들을 소개하고 이를 이용한 실험결과를 제시하였다.

Ⅰ. 서론

인터넷과 같은 컴퓨터 망과 컴퓨터 이용의 급격한 발달로 인하여 문서, 음성, 오디오, 영상, 동영상 등의 멀티미디어 데이터의 이용 및 보급이 일반화 되고있다. 그러나 이러한 멀티미디어 데이터들은 디지털이라는 속성으로 인하여 복사를 하게 되면 또 하나의 원본이 만들어지게 되므로 누구나 손쉽게 불법적인 복제를 통해서 이들 디지털 데이터를 획득할 수 있게 된다.

지금까지 가장 대표적이고 널리 사용되는 데이터 보호기법은 데이터를 암호화 하는 방법으로 암호를 알지 못하면 데이터에 접근이 불가능하다는 장점이 있다. 하지만 일단 암호가 해독된 데이터는 아무런 제재 없이 불법적으로 복사되고 배포될 수 있다는 문제점을 가지고 있다. 이와 같은 이유로 인해서 최근에 디지털 워터마킹 기법이 디지털 멀티미디어 컨텐츠 저작권 보호를 위한 새로운 해결책으로 제시되고 있으며, 국내외에서 이와 관련된 연구가 활발히 진행되고 있다[1-5].

본 논문에서는 멀티미디어 컨텐츠 보호를 위해 사용되는 대표적인 워터마킹 기법들을 소개하였다. 멀티미디어 컨텐츠의 속성상 각각의 컨텐츠는 각기 다른 방법으로 워터마크가 내장되어야 하므로 워터마킹 기법들을 문서, 영상, 그리고 오디오에 따라 분류하고 이들에 대한 실험을 수행하였다.

Ⅱ. 문서 데이터의 워터마킹

문서 데이터의 워터마킹은 전자문서 형태로 저장된 2진 영상을 위주로 하여 주로 연구되어져 왔고 최근들어 OCR(optical character recognition)기술과 결합되어 그 응용 범위가 더욱 확대되어 왔다. 문서 데이터 워터마킹의 대표적인 응용으로는 최근에 널리 이용되고 있는 가상 디지털 도서관(virtual digital library)의 경우가 이에 해당한다.

문서 데이터 워터마킹 기법은 Brassil[6]에 의해 광범위하게 연구되어졌는데 대표적인 문서 데이터 워터마킹 기법으로는 라인 천이 부호화(line shift coding), 단어 천이 부호화(word shift coding), 그리고 특징 부호화(feature coding) 방법이 있다. 라인 천이 부호화는 문서에 있는 라인들의 간격을 위와 아래로 조금씩 이동시키는 방법이다. 이때 문서에 저장되게 되는 워터마크 정보는 각각의 라인이 움직인 방법에 의해 결정되게 된다. 단어 천이 부호화의 경우

에는 라인 천이 부호화와 유사하게 단어들 사이의 공간을 조정하여 워터마크 정보를 내장하게 되는 기법이다. 특징 부호화 방법은 문서에서 특정 문자들의 모양을 특징으로 선정하여 이들의 모양을 약간씩 변형시켜 워터마크 정보를 내장 시킨다.

Ⅲ. 영상 데이터의 워터마킹

가. 공간영역에서의 워터마킹

이 방법은 공간영역에서 영상 데이터를 표현하는 각각의 픽셀(pixel)값을 이진수로 표현한 다음 이 중 LSB(Least Significant Bit)에 워터마크를 직접 내장하는 방법이다[2]. LSB 에 워터마크를 내장하는 이유는 워터마크를 내장한 후에 발생할 수 있는 영상의 열화를 최소화 하기 위해서이다. 이 알고리즘에서 이진수로 표현된 픽셀에 내장되는 워터마크는 당연히 이진수로 표현되어야 한다. 워터마크 검출시에는 미리 저장된 워터마크와 워터마크가 내장된 영상에서 추출한 추정된 워터마크 간에 상관관계를 이용하여 실제 워터마크가 내장 되었는지를 판단하게 된다.

나. 주파수영역에서의 워터마킹

현재 대다수의 워터마킹 알고리즘은 DCT (discrete Cosine Transform)나 DWT(discrete wavelet transform)과 같은 주파수영역에서 워터마크를 삽입하고 있다[7-13]. 과거의 워터마킹 기술이 알고리즘의 비공개에 주로 의존해 온 반면 Cox[7]의 방식은 알고리즘을 공개할 수 있다는 점에서 기술적으로 큰 변화를 가져온 계기가 되었다. 이 방식에 있어서 워터마크란 백색잡음을 의미하고 이 백색잡음은 슈도랜덤수(pseudo-random number)이다. 이 슈도랜덤수를 발생시키는 seed 가 워터마크를 찾아내는 키(key) 역할을 한다. Cox 의 방법은 워터마크 검출시 원영상과의 차를 이용한다는 점에서 약점이 존재하지만, 이 방식은 현재 연구되고 있는 대부분의 워터마킹 기술에서 수정되어 사용되고 있다.

워터마크 $w(n)$는 다음 식(1)과 같이 자기상관함수가 임펄스 형태인 백색잡음이다.

$$R_{ww}(\tau) \equiv E[w(n+\tau)w(n)] = \sigma_w^2\delta(\tau) \quad (1)$$

워터마크의 삽입 시 워터마크의 크기는 영상의 신호에 비해 상대적으로 굉장히 작도록 설정하여야 한다. 또한 원영상의 주파수 성분 중, 크기가 큰 주파수 성분에 워터마크의 크기를 크게 삽입하고, 크기가 작은 주파수 성분에는 워터마크의 크기를 작게 삽입한다. 즉,

$$w'(n) = \alpha \mid X(n) \mid w(n) \quad (2)$$

여기서, α는 상수이고 $X(n)$은 워터마크를 삽입하고자 하는 영상 신호의 n 번째 주파수 성분이다.

그리고, 워터마크가 삽입되는 주파수 영역은 공격에 강하고 공격이 가해졌을 때 영상 신호의 화질을 크게 손상시킬 수 있는 영역이어야 한다. 고주파 대역에 워터마크가 삽입될 경우 공격으로부터 쉽게 워터마크가 제거될 수 있다. 또는 압축 알고리즘을 통해서도 쉽게 손상될 수 있다. 반면, 저주파 대역에 워터마크를 삽입할 경우, 워터마크를 제거하기 위해서는 저주파 대역에 왜곡을 가해야 한다. 이는 영상 신호의 주파수 성분들이 저주파대역에 집중되어 있어 영상 화질에 큰 저하를 가져온다. 따라서 영상을 2 차원 DCT 를 수행한 후 저주파 대역이면서 주파수 성분의 크기가 큰 N 개의 성분에 대해 워터마크를 삽입한다.

$$X'(n) = X(n) + \alpha \mid X(n) \mid w(n) \quad (3)$$

여기서 $X'(n)$은 워터마크가 삽입된 주파수 영역에서의 원영상 신호이다.

워터마크의 검출은 워터마크가 삽입된 신호와 워터마크 사이의 상관성을 구함으로써 쉽게 이루어질 수 있다. 그림 1 은 워터마크의 검출과정을 나타낸 것이다. 그림 2(a)는 원본 lenna 영상이며, 2(b)는 Cox 의 알고리즘을 이용하여 워터마크를 내장한 영상이다. 두 영상의 시각적인 차이를 거의 느낄 수 없다. 그림 2(c)와 2(d)는 Cox 알고리즘에 공격을 가했을 경우에 대한 예를 보여주고 있다. 그림 2(c)는 워터마크가 내장된 영상을 150×150 으로 decimation 한 후 다시 원래의 크기인 256×256

으로 선형보간 한 후의 유사도(similarity)를 나타내고 있다. 그림 2(d)는 가우시안 잡음을 첨가한 후 저대역통과필터를 거친 경우를 보여주고 있다. 공격이 가해진 영상에서 워터마크 알고리즘이 얼마나 강인한가를 판별하는 척도는 유사도의 값이 얼마나 크게 나왔느냐에 달려있다.

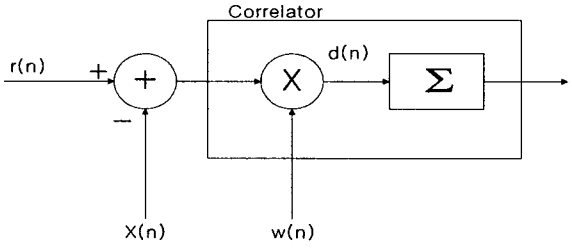
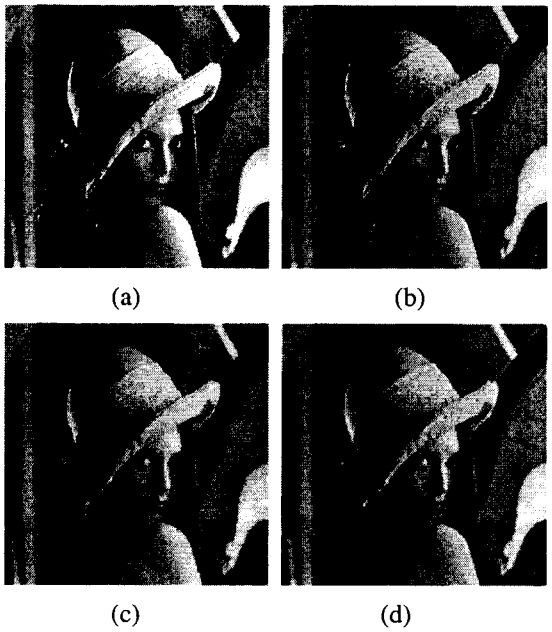


그림 1. 워터마크의 검출



(a) 원본영상
(b) 워터마킹된 영상 (유사도: 30.12)
(c) Resized(150×150) 영상 (유사도: 23.76)
(d) Gaussian noise + lowpass filtering (유사도: 21.70)

그림 2. 워터마크가 내장된 영상 및 공격이 가해진 경우의 워터마크 검출 예

Ⅳ. 오디오 데이터의 워터마킹

현재까지 발표된 워터마크 알고리즘의 대다수는 영상데이터를 대상으로 하였고, 오디오 데이터를 대상으로 한 경우는 극히 일부에 지나지 않는다. 하지만 최근 들어 문제가 되고 있는 MP3 오디오 파일의 불법복제 등을 생각해 볼 때 오디오 데이터의 워터마킹 기법 역시 시급히 해결되어야 할 과제이다.

최근까지 연구된 오디오 데이터 워터마킹 방식 중 공격에 강하면서도 상대적으로 오디오의 품질을 손상 시키지 않는 것으로 알려진 방식은 인간의 청각특성을 이용하는 방법이다. 즉, 마스킹 곡선을 이용함으로써 워터마크가 삽입된 후에도 오디오 데이터의 품질을 떨어뜨리지 않게 되며 임의의 공격에도 강인한 특성을 지니게 된다[14]. 전체적인 알고리즘은 다음과 같다.

1) 오디오 신호를 일정크기의 처리 단위인 프레임으로 나눈다.
2) 프레임 단위의 오디오 데이터의 전력 스펙트럼을 구한다.
3) 구해진 스펙트럼 에서 순음과 잡음성분을 구한다.
4) 가청한계곡선 이하의 성분을 제거한다.
5) 각각의 순음 성분과 잡음 성분에 대한 마스킹 곡선을 구한다.
6) 구해진 각각의 마스킹 한계치를 이용하여 전체적인 마스킹 곡선를 구한다.
7) 프레임 길이와 동일한 랜덤신호를 발생시킨 후 전력 스펙트럼을 구한다음 미리구해진 오디오 신호의 마스킹 곡선과 곱한 다음 역변환 하여 시간영역의 워터마크를 구한다.
8) 구해진 워터마크를 오디오 신호에 더하여 삽입한다.

그림 3 은 전체적인 워터마킹 과정을 나타내고 있다. 이 방법에서 워터마크의 검출과정은 앞 절에서 설명한 Cox 의 방법과 동일하다. 그림 4 는 앞서 설명한 알고리즘을 이용하여 워터마킹된 오디오 데이터에 공격이 가해졌을 경우에 대한 결과이다. 그림에서 watermark A

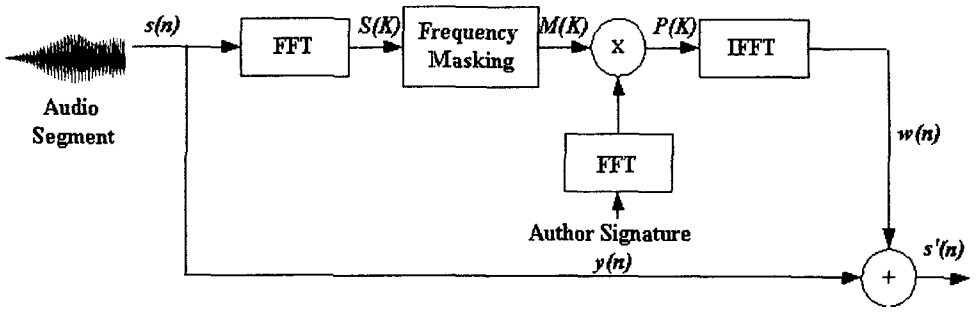
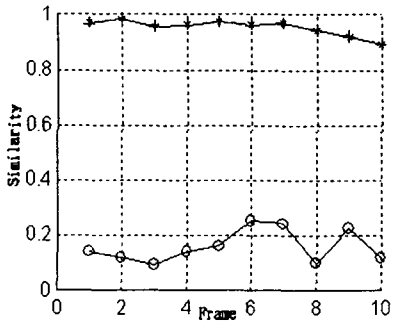


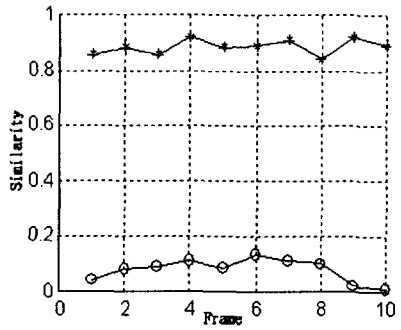
그림 3 오디오 워터마킹 과정

는 실제로 오디오 데이터에 삽입된 워터마크를 이용하여 검출한 결과를 나타내며 watermark B 는 삽입된 워터마크와 다른 워터마크로 검출한 결과를 각각 나타내고 있다.

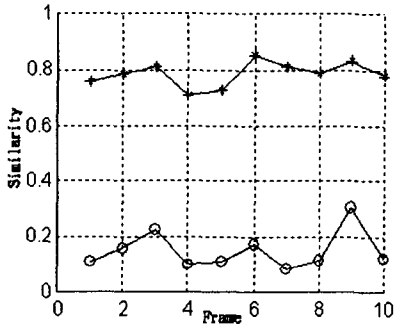
공격으로 사용된 방법으로 Band-pass filtering, Down sampling, Time scale modification, Low bit-rate coding 의 네 가지 경우를 사용하였다. 그림에서도 확인할 수 있듯이 Band-pass filtering, Down sampling, Time scale modification 의 경우에는 삽입된 워터마크를 안정적으로 검출할 수 있었다. 하지만 Low bit-rate coding 방식인 MPEG2 AAC 를 이용하여 공격이 가해졌을 경우 상대적으로 검출이 까다로움을 확인할 수 있었다. 이는 워터마킹 알고리즘에서 사용한 심리음향 모델과 MPEG2 AAC 에서 사용한 심리음향 모델이 서로 다르기 때문이라 생각되며 이 외에도 MPEG 2 AAC 에서는 여러 가지 신호처리적인 기법들이 사용되어서 신호 자체에 많은 변형이 생겨서 다른 공격에 비해 상대적으로 검출이 어려웠다.



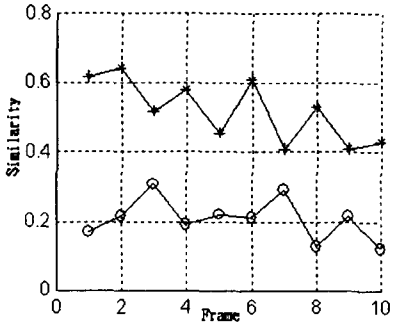
(a) Band-pass filtering (100-6k Hz, 2nd order Butterworth filter)



(b) *Time scale modification (+4%)*



(c) Down Sampling (44.1→22.05 kHz)



(d) Low bit rate coding (MPEG2 AAC Mono 64kbps)

그림 4. 워터마크가 내장된 오디오에 공격이 가해진 경우의 워터마크 검출 예
(* : watermark A, o : watermark B)

V. 결론

본 논문에서는 멀티미디어 데이터의 소유권을 보호할 수 있는 문자, 영상 및 오디오 데이터의 워터마킹 기술에 대해 살펴 보았다.

지금까지 연구된 워터마킹 기술의 경우 부분적으로는 임의의 공격에 견딜 수 있으며 지각적으로도 양호한 결과를 보인다고 발표되고 있다. 하지만 현재까지 모든 조건을 만족하는 강인한 워터마크 알고리즘은 앞으로 많은 기술적 발전이 있어야 가능할 것으로 판단된다.

참고문헌

[1] F. Hartung, M. and Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1079-1107, July 1999.

[2] A. Tirkel et al., "Electronic water mark," in *Proc. DICTA 1993*, pp. 666-672, Dec. 1993.

[3] F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1062-1078, July 1999.

[4] M. D. Swanson et al., "Transparent robust image watermarking," *Proc. ICIP'96*, Vol. 3, pp. 211-214, 1996.

[5] R. Wolfgang and E. J. Delp, "Watermark for digital image," *Proc. ICIP'96*, Vol. 3, pp. 219-222, 1996.

[6] J. Brassil et al., "Electronic marking and identification techniques to discourage document copying," *IEEE J. Select. Areas Commun.*, Vol. 13, pp. 1495-1504, Oct. 1995.

[7] I. Cox et al., "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing*, Vol. 6, No. 12, pp. 1673-1687, Dec. 1997.

[8] W. Zeng and B. Liu, "On resolving rightful ownership of digital images by invisible watermarks," *Proc. ICIP'97*, Vol. 1, pp. 552-555, 1997.

[9] K. Ratakonda et al., "Digital image watermarking : issues in resolving rightful ownership," *Proc. ICIP'98*, pp. 414-418, 1998.

[10] M. Barni et al., "DCT-domain system for robust image watermarking," *Signal Processing*, Vol. 66, No. 3, pp. 357-372, May 1998.

[11] I. Pitas, "A method for signature casting on digital images," *Proc. ICIP'96*, Vol. 3, pp. 215-218, 1996.

[12] A. Piva et al., "DCT-based watermark recovering without resorting to the uncorrupted original image," *Proc. ICIP'97*, Vol. 1, pp. 520-523, 1997.

[13] J. J. O. Ruanaidh et al., "Phase watermarking of digital images," *Proc. ICIP'96*, Vol. 3, pp. 239-242, 1996.

[14] M. Swanson et al., "Robust audio watermarking using perceptual masking," *Signal Processing*, Vol. 66, No. 3, pp. 337-355, May 1998.