가역 워터마킹을 이용한 블록 단위 오디오 인증 알고리즘

여동규*, 조현우*, 이해연*
*국립금오공과대학교 컴퓨터소프트웨어공학과
e-mail:sylot@kumoh.ac.kr

Block-based Audio Authentication Algorithm using Reversible Watermarking

Dong-Gyu Yeo*, Hyun-Wu Jo*, Hae-Yeoun Lee*
*Dept. of Computer Software Engineering, Kumoh National Institute of Technology

요 약

데이터 은닉 기술은 디지털 콘텐츠에 기밀 정보를 비가시적으로 삽입하는 기술로서, 소유권 증명, 저작권 보호, 방송 모니터링, 콘텐츠 인증 등의 다양한 목적으로 활용되고 있다. 본 논문에서는 오디오 콘텐츠의 무결성을 인증하고 위조 영역을 탐지하기 위한 가역 워터마킹 기반의 블록 단위의 오디오 콘텐츠 인증 기법을 제안한다. 제안한 기법은 오디오를 작은 크기의 블록으로 나누고 각 블록 단위로 워터마크를 삽입하여 무결성 인증을 수행한다. 또한 차이값 히스토그램 기반 가역 워터마킹 알고리즘을 적용함으로써 높은 품질을 유지하면서도 완전한 원본으로의 복원을 가능케 하였다.

1. 서론

데이터 은닉 기술은 음악, 영상, 동영상, 전자문서, 교육자료, 애니메이션과 같은 디지털 콘텐츠에 기밀 정보를 비가시적으로 삽입하는 기술로서, 소유권 증명, 저작권 보호, 방송 모니터링, 콘텐츠 인증 등의 다양한 목적으로 활용되고 있다. 또한 응용에 따라 다양한 삽입용량과 지각적 투명성, 강인성, 기밀성, 계산 복잡도 등의 요구조건을 만족시킬 수 있다.

콘텐츠에 데이터를 은닉하려면 필연적으로 원본 콘텐츠의 수정이 불가피한데, 의료 및 군사용 콘텐츠, 법률적 증거, 원격 측정값, 예술작품 등의 응용분야에서는 어떠한 손상도 없는 원본 콘텐츠가 필요하다. 연성(Fragile) 워터마킹의 한 종류인 가역(Reversible) 워터마킹은 워터마킹된 콘텐츠에서 메시지를 제거한 후 원본 콘텐츠로 완전한 복원이 가능하며, 아주 작은 변형만으로도 쉽게 워터마크가 손상되기 때문에 콘텐츠의 위조 및 변조에 대한 무결성 인증에 유용하게 적용될 수 있다.

인간의 심리 음향 모델을 이용하여 원본과의 차이를 느끼지 못할 정도의 품질저하를 통해 메시지를 삽입하는 기존의 오디오 워터마킹 연구들[1-5]은 삽입한 워터마크의 강인성에 초점을 맞추었기 때문에 워터마크의 제거 후에 원본 복원이 불가능한 것이 많고, 위변조에 대한 탐지 정확도 또한 높지 않았다. 따라서 반드시 원본 콘텐츠가 필요한 분야에서 사용하기에는 어려움이 있었다. 또한 콘텐츠의 무결성 인증을 할 때, 전체 콘텐츠에 대하여 위변조 여부를 판별하기보다는 어느 영역이 위변조 되었는지 탐지하는 것이 실제 응용에서 더 유용할 수 있다. 본 논문에서는 오디오 콘텐츠의 무결성을 인증하고 위조 영역을 탐지하기 위한 가역 워터마킹 기반의 오디오 콘텐츠 인증 기법을 제안한다. 제안한 기법은 오디오를 작은 크기의 블록으로 나누고 각 블록 단위로 워터마크를 삽입하여 무결성 인증을 수행한다.

· 본 연구는 문화체육관광부 및 한국저작권위원회의 2011년도 저작권기술개발사업의 연구결과로 수행되었음.

2. 오디오 인증 알고리즘

오디오 콘텐츠 전체에 대한 한 번의 위변조 판별이 아닌 블록 단위의 인증을 수행하기 위해서는 블록 단위의 특징을 추출하여야 하며, 인증 확인 역시 블록 단위로 행해져야만 한다. 따라서 본 논문에서는 오디오 콘텐츠를 블록 단위로 분할하여, 각 블록 단위의 인증 정보 생성 및 삽입을 수행한다. 수신된 오디오에 대해서는 삽입된 인증 정보를 검출하고, 복원된 오디오에 대해서 인증 정보를 재생성하여 비교함으로써 위변조 여부를 판별할 수 있다.

블록 단위로 인증정보를 삽입하는 전체적인 절차는 다음과 같으며, 3절의 가역 워터마킹 방법을 이용하여 삽입한다.

(가) 오디오를 블록 단위로 분할
(나) 각 블록 단위의 인증정보 생성
(다) 각 블록 단위로 인증정보 삽입

오디오의 무결성을 인증하기위한 전체적인 절차는 다음과 같으며, 3절의 가역 워터마킹 방법을 이용하여 삽입된 인증정보를 검출한다.

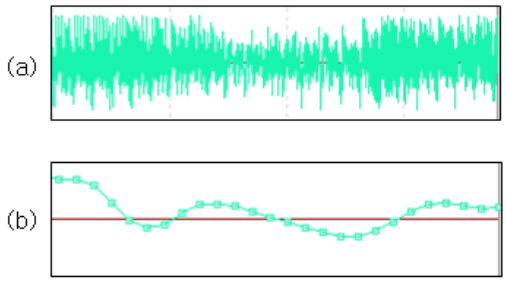
(가) 오디오를 블록 단위로 분할
(나) 인증정보를 검출하고 제거하여 오디오를 복원
(다) 인증정보를 재생성
(라) 검출한 인증정보와 재생성한 인증정보를 비교

고성능의 인증률을 달성하기 위해서는 오탐지의 확률을 최소화하기 위한 충분한 길이의 인증코드를 사용하여야 한다. 본 논문에서는 각 블록의 특징을 구분하기 위하여 해시값을 사용하였는데, 실험적으로 얻은 최적의 인증코드 길이는 16비트로서 이것의 우연에 의한 오탐지 확률은 1/(2^16)가지 즉, 1/65536 = 1.52588E-05의 확률이므로 그 가능성은 매우 낮다고 할 수 있을 것이다. 블록의 인증코드로는 해시값 뿐만 아니라, 알고리즘을 적용할 응용에 따라 사용자에 특화된 고유ID/비밀번호/기관코드/오디오생성장치ID/타임코드/비밀키 등을 응용목적에 따라 유연하게 사용할 수 있으며, 정확도를 높이기 위하여 인증코드의 길이를 더 길게 사용할 수도 있다.

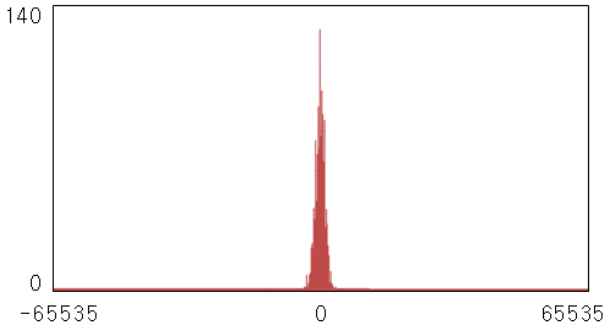
3. 가역 워터마킹 기반 인증정보 삽입 및 검출

히스토그램 쉬프팅 기법을 이용하는 가역 워터마킹 알고리즘들은 데이터를 삽입하려는 최대점 주위의 히스토그램을 수정하여 빈 공간을 확보하고 확보된 공간에 최대점을 분산시키는 방법을 사용하여 데이터를 삽입한다. 따라서 높은 데이터 삽입용량을 얻기 위해서는 최대점들을 많이 확보해야 한다. 하지만, 많은 최대점들을 사용할수록 원본 콘텐츠의 왜곡이 심해지고 오버헤드 정보의 양과 알고리즘의 복잡도가 증가한다. 반면 차이값 히스토그램을 이용하면 하나의 최대점만 사용하더라도 높은 삽입용량을 얻을 수 있다.

차이값 히스토그램은 인접한 샘플과의 차이값를 이용하여 계산한다. 그림 1-(a)와 같이 일반적인 오디오 파형을 보면 진폭의 차이가 심하게 보이지만, 그림 1-(b)처럼 확대하여 살펴보면 값들의 지역성이 높음을 알 수 있다. 그림 2에 임의의 0.1초 블록에 대한 차이값 히스토그램을 보였는데, 대부분의 차이값이 0 주변에 몰려있음을 확인할 수 있다. 높은 최대점을 갖는 것은 적은 왜곡으로 높은 삽입용량을 얻을 수 있다는 것을 의미하므로, 차이값 히스토그램을 이용하는 것이 유리하다. 또한 일반 히스토그램을 이용한 방법은 데이터 삽입 후 최대점의 위치가 변하기 때문에 원래의 최대점의 위치를 기억하기 위한 추가적인 오버헤드가 발생한다. 하지만 차이값 히스토그램을 이용한 방법은 인접한 샘플간의 변화가 작다는 지역성 특징으로 인하여 차이값들이 0 주변으로 몰려있기 때문에 최대점의 위치를 고정시켜서 처리할 수 있으므로 삽입위치 정보에 대한 오버헤드가 필요하지 않다는 장점을 가진다.



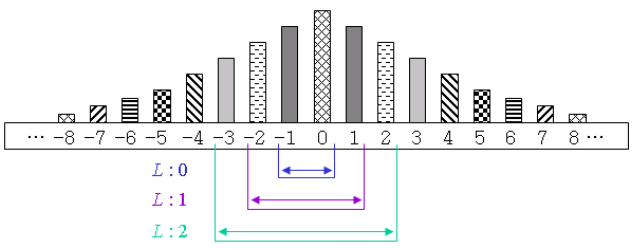
(그림 1) 오디오 파형: (a)확대 전, (b)확대 후



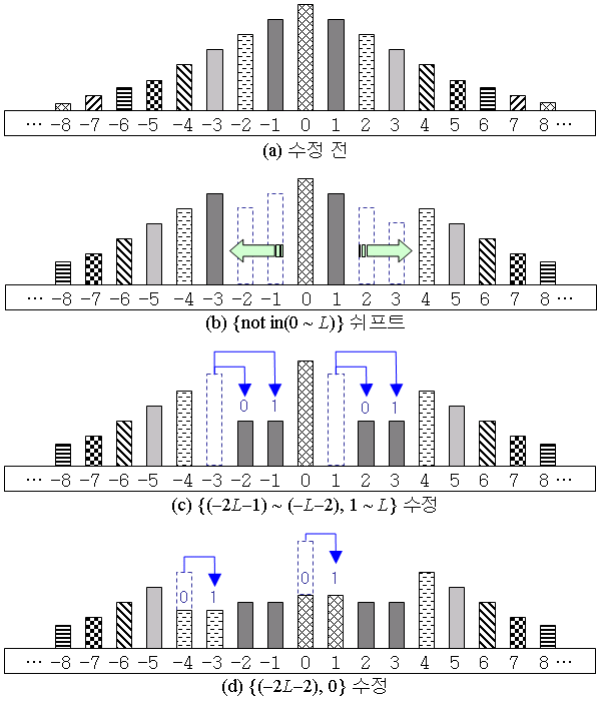
(그림 2) 0.1초 길이 블록에 대한 차이값 히스토그램

본 논문에서는 각 블록단위로 인증정보를 삽입 및 검출하기 위하여, 영상 콘텐츠 인증을 위하여 개발된 [6] 연구의 차이값 히스토그램 기반 가역 워터마킹 알고리즘을 변형하여 사용하였다.

본 논문에서 삽입해야할 블록별 인증코드의 길이는 16비트이므로 블록의 삽입가능 용량이 충분한지 확인하여야 한다. 삽입되는 메시지의 용량 및 워터마킹된 콘텐츠의 품질은 삽입레벨 L 로 조절한다. 0부터 시작되는 L의 값에 따라 차이값 히스토그램에서 메시지 삽입에 이용되는 빈은 0번 빈 주위인 {(-L-1)~(+L)}까지로서 그림 3에 나타내었다. 따라서 L의 값을 0부터 1씩 증가시키며 삽입가능한 용량을 확인하여 인증정보를 삽입할 수 있는 삽입레벨을 알아낸다.



(그림 3) 메시지 삽입에 이용되는 히스토그램 빈



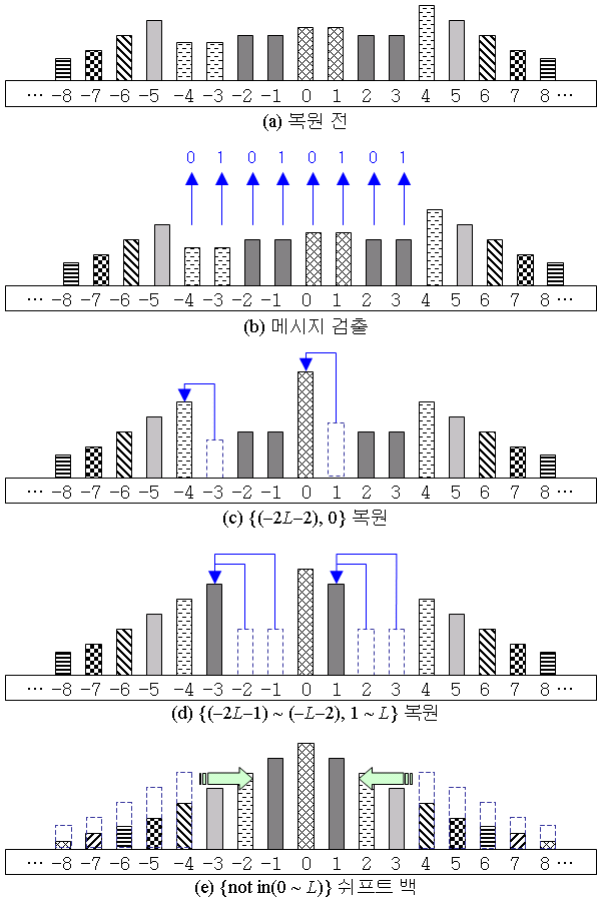
(그림 4) 인증코드 삽입과정에서의 히스토그램 수정 절차 (삽입레벨 L=1의 경우)

삽입레벨 L이 1인 경우 메시지가 삽입되는 과정에서 히스토그램이 수정되는 절차를 그림 4에 나타내었다. 먼저 원본 오디오에 대하여 점진적으로 차이값 히스토그램을 구성한 후, 삽입공간을 확보하기 위하여 삽입에 이용되지 않는 빈들을 쉬프트한다. 다음으로 삽입할 메시지의 비트에 따라 히스토그램을 수정하고, 수정된 히스토그램을 반영한 은닉 오디오를 만들어 낸다.

워터마킹된 메시지를 검출하기 위해서는 삽입과정을 역순으로 진행하면 되는데, 삽입레벨 L이 1인 경우 메시지를 검출하고 원본 오디오를 복원하는 과정에서 히스토그램이 수정되는 절차를 그림 5에 나타내었다. 먼저 은닉 오디오에 대하여 점진적으로 차이값 히스토그램을 구성한 후, 메시지 삽입공간을 스캔하여 삽입된 메시지를 검출한다. 다음으로 메시지를 삽입하기 위하여 수정되었던 히스토그램을 복원하고, 공간확보를 위하여 쉬프트되었던 빈들을 복원한다. 마지막으로 복원된 히스토그램을 이용하여 원본 오디오를 복원하게 된다.

4. 실험 및 성능 평가

다양한 장르의 7곡을 선정하여 실험에 사용하였으며, 오디오 데이터 파일의 형식은 16KHz 샘플링레이트의 16bit 샘플 Mono PCM Wave이다. 정밀한 인증을 수행하기 위하여 0.1초 단위로 인증실험을 수행하였다. 인증정보가 삽입된 오디오 콘텐츠의 품질은 다음 수식 1의 SNR (The signal-to-noise ratio) 측정방식을 이용하였다. $x_{(n)}$은 원본 오디오 콘텐츠이며, $x'_{(n)}$은 워터마킹된 오디오 콘텐츠이다.



(그림 5) 메시지 검출 및 복원과정에서의 히스토그램 수정 절차 (삽입레벨 L=1의 경우)

$$SNR = 10 \cdot \log_{10} \frac{\sum_{\forall n} (x_{(n)})^2}{\sum_{\forall n} (x_{(n)} - x'_{(n)})^2} \quad (1)$$

워터마킹된 오디오 콘텐츠에 대하여 볼륨 조절 및 에코 추가 공격을 가하고, 인증 확인을 수행한 결과를 표 1에 나타내었다. 샘플 값들의 지역성이 높기 때문에 모든 실험 오디오에 대하여 삽입레벨은 0으로 충분하였다. 또한 평균 84.72의 높은 품질을 보여 원본과의 차이가 거의 없었으며, 거의 모든 공격 블록에 대하여 위변조를 탐지할 수 있었다.

<표 1> 오디오 워터마킹 및 인증 실험결과

오디오	삽입레벨	SNR(dB)	인증률(%)
Clip01	0	83.51	100.0
Clip02	0	83.34	100.0
Clip03	0	83.66	99.7
Clip04	0	87.87	99.3
Clip05	0	84.59	100.0
Clip06	0	87.08	100.0
Clip07	0	82.97	99.6
평균	0	84.72	99.8

5. 결론 및 향후연구방향

본 논문에서는 오디오 콘텐츠의 무결성을 검증하기 위한 알고리즘으로서, 원본 오디오를 블록단위로 분할하여 각 블록에 인증정보를 삽입함으로써 공격자에 의한 손상 여부를 인증할 수 있는 기법을 제안하였다. 인증코드를 삽입하는 알고리즘은 점진적 차이값 히스토그램을 수정하는 방법을 이용하였다. 특히 영상 콘텐츠에 대한 워터마킹 알고리즘으로 개발된 차이값 히스토그램 방법을 오디오 워터마킹에도 성공적으로 적용할 수 있음을 보였다. 또한 0.1초 단위의 인증을 수행함으로써 정밀한 위변조 탐지를 가능케 하였다. 다양한 실험 데이터들을 이용하여 실험한 결과, 높은 청각적 품질을 유지하면서도 고속으로 인증코드를 삽입 및 검출/인증할 수 있음을 확인하였다.

향후 지속적인 연구를 통하여 다양한 샘플링레이트의 오디오 콘텐츠에 적용 가능할 뿐만 아니라, 상용 음악 파일 형식인 MP3와 같은 압축형식에 적합하게 확대할 필요가 있다.

참고문헌

[1] Z. Liu, Y. Kobayashi, S. Sawato and A. Inoue, "A robust audio watermarking method using sine function patterns based on pseudo-random sequences," Proc. of Pacific Rim Workshop on Digital Steganography 2002, pp. 167-173, 2002

[2] S. Liu, S.D. Lin, "BCH Code-based Robust Audio Watermarking in the Cepstrum Domain," Journal of Information Science and Engineering, 2006, 22:535-543

[3] S. Xiang, J. Huang and R. Yang, "Time-scale Invariant Audio Watermarking Based on the Statistical Features in Time Domain," Proc. of the 8th Information Hiding Workshop, 2006.

[4] S. Xiang, H.J. Kim, "Invariant Audio Watermarking in DWT Domain," The 1st International Conference of Ubiquitous Information Technology, 2007.

[5] X. Zhang, X. Yin and Z. Yu, "Histogram Specification-based Audio Watermarking Technology against Filtering Attacks in Time Domain," International Symposium on Electronic Commerce and Security, pp. 951-956, 2008

[6] 여동규, 이해연, "차이값 히스토그램 기반 가역 워터마킹을 이용한 블록 단위 영상 인증 알고리즘", 정보처리학회논문지, 2011 (accepted)