http://dx.doi.org/10.3745/KIPSTB.2012.19B.1.009

가역 워터마킹을 이용한 구간 단위 오디오 무결성 인증 알고리즘

여 동 규[†] · 이 해 연[††]

요 약

콘텐츠의 인증을 위한 기존의 오디오 워터마킹 연구들은 워터마크의 제거 후에 원본 복원이 불가능한 것이 많다. 가역 워터마킹 기법은 고신뢰성의 오디오 콘텐츠가 요구되는 응용분야에서 오디오 데이터의 무결성을 인증하기 위한 효과적인 방법으로 적용될 수 있다. 가역 워터마킹 기법은 디지털 콘텐츠에 지각적 투명성을 유지하며 워터마크를 삽입한 후, 이를 아무런 손상없이 원본 상태로 복원할 수 있게 한다. 본 논문에서는 악의적인 위변조를 탐지하는 구간 단위의 오디오 무결성 인증 알고리즘을 제안하며, 완전한 가역성을 제공하기 위하여 차이값 히스토그램 기반 가역 워터마킹 기법을 사용한다. 전체에 대해서 한 번의 인증이 아닌 부분적인 인증을 위하여 오디오를 구간 단위로 분할하여 인증 정보를 삽입하며, 무결성 인증 또한 구간 단위로 수행된다. 다양한 실험 데이터들에 대하여 비교 분석한 실험 결과에 따르면 제안한 알고리즘은 완전한 가역성과 함께 낮은 왜곡을 유지하면서도 99% 이상의 높은 인증률을 얻을 수 있었다.

키워드 : 오디오 인증, 오디오 워터마킹, 가역 워터마킹

Interval-based Audio Integrity Authentication Algorithm using Reversible Watermarking

Dong-Gyu Yeo[†] · Hae-Yeoun Lee[††]

ABSTRACT

Many audio watermarking researches which have been adapted to authenticate contents can not recover the original media after watermark removal. Therefore, reversible watermarking can be regarded as an effective method to ensure the integrity of audio data in the applications requiring high-confidential audio contents. Reversible watermarking inserts watermark into digital media in such a way that perceptual transparency is preserved, which enables the restoration of the original media from the watermarked one without any loss of media quality. This paper presents a new interval-based audio integrity authentication algorithm which can detect malicious tampering. To provide complete reversibility, we used differential histogram-based reversible watermarking. To authenticate audio in parts, not the entire audio at once, the proposed algorithm processes audio by dividing into intervals and the confirmation of the authentication is carried out in each interval. Through experiments using multiple kinds of test data, we prove that the presented algorithm provides over 99% authenticating rate, complete reversibility, and higher perceptual quality, while maintaining the induced-distortion low.

Keywords : Audio Authentication, Audio Watermarking, Reversible Watermarking

1. 서 론

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. 암호화 기술도 디지털 콘텐츠 보호를 위한 방법이지만 그것은 콘텐츠 배포과정에서의 보호만 보장할 뿐이며, 한 번 복호화된 콘텐츠는 더 이상 보호될 수 없기 때문에 콘텐츠의 무결성을 입증하기 위한 충분한 수단을 제공하기에는 부족하다. 이에 반하여 데이터 은닉 기술은 응용에 따라 다양한 삽입용량과 지각적 투명성, 강인성, 기밀성, 계산 복잡도 등의 요구조건을 만족시킬 수 있다.

대표적인 데이터 은닉 기술인 디지털 워터마킹은 삽입될 메시지와 원본 콘텐츠가 밀접한 연관성을 가지고 있는데,

※ 본 연구는 문화체육관광부 및 한국저작권위원회의 2011년도 저작권 기술개발사업의 연구결과로 수행되었음.
† 정 회 원 : 국립금오공과대학교 모바일연구소 박사후연구원
†† 정 회 원 : 국립금오공과대학교 컴퓨터소프트웨어공학과 교수(교신저자)
논문접수 : 2011년 10월 25일
수 정 일 : 1차 2012년 1월 3일
심사완료 : 2012년 1월 5일

원본 콘텐츠에 대한 메타데이터 혹은 무결성 검증을 위한 인증코드, 저작권 정보 등이 워터마크의 내용이 될 수 있다. 워터마킹은 응용 관점에 따라 강인성(Robust) 워터마킹과 연성(Fragile) 워터마킹으로 분류된다[1]. 강인성 워터마킹은 콘텐츠의 지각적 품질을 유지하면서 모든 가능한 왜곡 시도로부터 워터마크의 내용이 보호될 수 있도록 설계된다. 반면 연성 워터마킹은 아주 작은 변형만으로도 쉽게 워터마크가 손상되기 때문에 콘텐츠의 위조 및 변조에 대한 무결성 입증이나 인증에 유용하게 적용될 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. 변경의 정도가 극히 미미하고 인간의 지각능력으로는 전혀 알아볼 수 없을지라도 올바른 결정에 영향을 미칠 수 있으며 법률적 문제가 될 수 있기 때문이다[2]. 연성 워터마킹의 한 종류인 가역(Reversible) 워터마킹은 워터마킹된 콘텐츠에서 메시지를 제거한 후 원본 콘텐츠로 완전한 복원이 가능하기 때문에 콘텐츠의 무결성 인증이나 위변조 조작에 대한 증명, 저작권 보호를 위한 용도로 이용되어질 수 있다[3].

기존의 오디오 워터마킹에 관한 연구들은 저작권 보호를 위한 응용에 이용하기 위하여 지각적 투명성 및 강인성 그리고 보안성 조건을 만족시키는 방향으로 연구되어졌다[4-5]. Haitsma et al.[6]은 퓨리에 변환 계수의 크기값을 수정하는 알고리즘을 제안하였는데, TSM(time-scale modification)과 MP3 압축 및 에코 추가 공격에 강인성을 보였지만 피치 쉬프팅(pitch shifting)에 약한 단점이 있었다. Kirovski et al.[7]은 스펙트럼 확산 워터마킹 방법을 이용하여 TSM 및 FSM(frequency-scale modification)에 강인한 결과를 보이지만 오탐지의 가능성이 있다. Tachibana et al.[8-9]은 이산 퓨리에 변환에서의 크기값을 수정하여 TSM에 강인하도록 설계하였으나 많은 시스템 자원을 필요로 하는 어려움이 있다. Mansour et al.[10-11]은 파형에서 두 개의 두드러지는 피크사이의 time-scale을 조정함으로써 TSM에 강인한 알고리즘을 제안하였으나 임계값 설정의 어려움이 있으며 피치 쉬프팅에 제한적이다. Li et al.[12]은 리듬의 변화가 분명한 오디오에 한정해서 적용할 수 있는 알고리즘을 제안하였다. Xiang et al.[13]은 샘플값 히스토그램과 평균값을 이용하여 TSM 및 잘라내기 공격에 강인한 알고리즘을 제안하였지만, 낮은 샘플링레이트에서는 강인성을 잃어버리는 문제가 있다. Zhang et al.[14]은 영화관 또는 콘서트장 등과 같은 공공장소에서 공중채널(Air channel)을 통해 녹음되는 오디오에 저작권 정보를 삽입하기 위하여 이중 DCT 계수를 수정하는 방법을 제안하였는데, 비록 공중채널 송신용에 국한되긴 하였지만 오디오 이용의 환경변화에 따른 새로운 응용가능성을 열었다. Huang et al.[15]은 위변조 탐지를 위한 데이터 은닉기법으로 DCT 스펙트럼의 고주파 영역을 MSB 방향으로 1비트씩 쉬프트한 후 LSB에 기밀정보를 삽입하는 알고리즘을 제안하였는데, 삽입된 영역 및 오버플로우로 인한 미삽입 영역의 위치를 기억하기 위한 별도의 위치정보맵을 필요로 하였다.

이와 같이 인간의 심리 음향 모델을 이용하여 원본과의 차이를 느끼지 못할 정도의 품질저하를 통해 메시지를 삽입하는 기존의 오디오 워터마킹 연구들은 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 구간으로 나누고 각 구간 단위로 워터마크를 삽입하여 무결성 인증을 수행한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 제안한 오디오 인증 알고리즘을 설명하고, 3장에서는 분할된 각 구단 단위의 오디오에 인증정보를 삽입하기 위한 가역 워터마킹 알고리즘 기반의 삽입 및 검출/복원 기법에 대하여 설명한다. 실험 및 성능 분석은 4장에서 제시하며, 5장에서 결론을 맺는다.

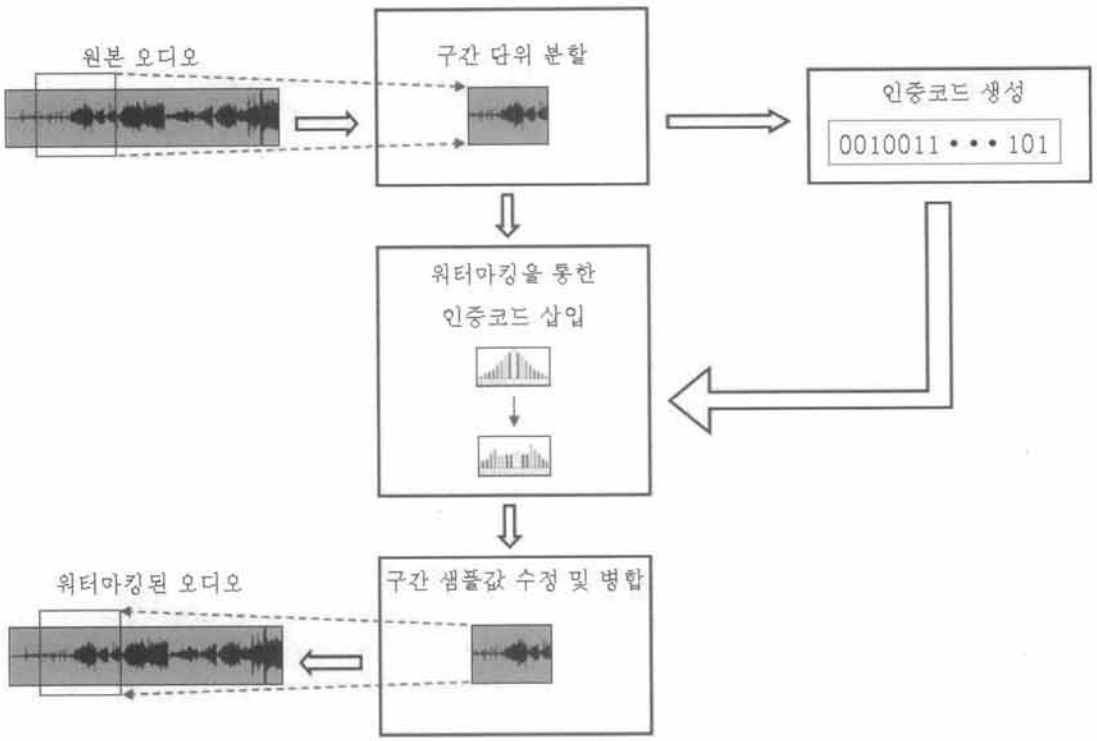
2. 제안하는 오디오 인증 알고리즘

오디오 콘텐츠 전체에 대한 한 번의 위변조 판별이 아닌 구간 단위의 인증을 수행하기 위해서는 구간 단위의 특징을 추출하여야 하며, 인증 확인 역시 구간 단위로 행해져야만 한다. 따라서 본 논문에서는 오디오 콘텐츠를 구간 단위로 분할하여 인증 정보를 생성하고, 구간 단위로 삽입을 수행한다. 인증정보를 삽입하는 전체적인 절차는 다음과 같으며 (그림 1)에 나타내었다. 개별 구간에 대한 인증정보 삽입은 3장의 가역 워터마킹 방법을 이용하여 삽입한다.

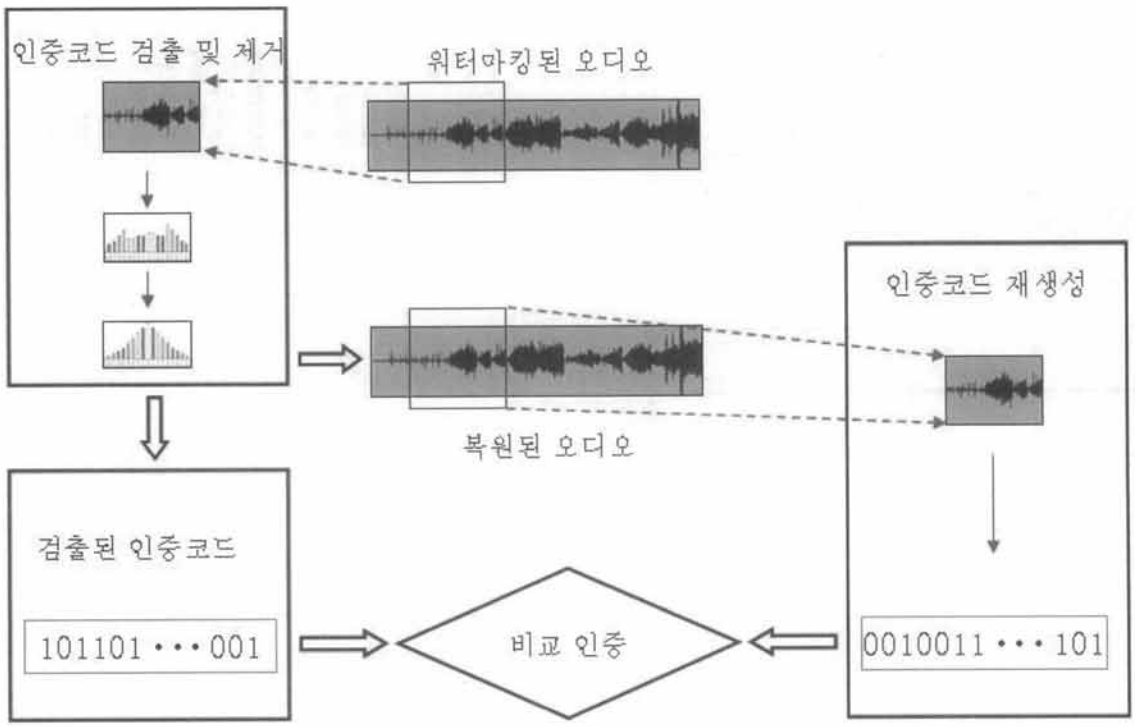
(가) 오디오를 구간 단위로 분할
(나) 각 구간 단위의 인증정보 생성
(다) 각 구간 단위로 인증정보 삽입

수신된 오디오에 대해서는 삽입된 인증 정보를 검출하고, 복원된 오디오에 대해서 인증 정보를 재생성하여 비교함으로써 위변조 여부를 판별할 수 있다. 오디오의 무결성을 인증하기위한 전체적인 절차는 다음과 같으며 (그림 2)에 나타내었다. 개별 구간에 대한 인증정보 검출 및 원본 복원은 3장의 가역 워터마킹 방법을 이용한다.

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



(그림 1) 인증정보 삽입절차



(그림 2) 인증정보 검출 및 인증 절차

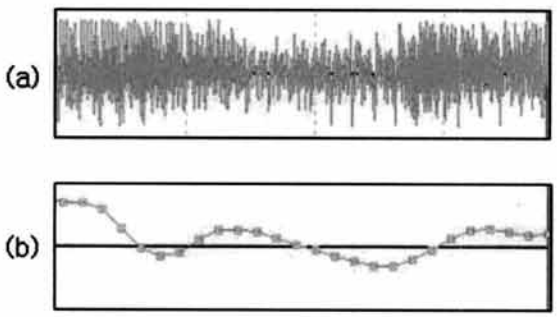
고성능의 인증률을 달성하기 위해서는 오탐지의 확률을 최소화하기 위한 충분한 길이의 인증코드를 사용하여야 한다. 인증코드가 너무 길면 콘텐츠의 품질저하가 심해지고, 너무 짧으면 우연에 의한 오탐지의 확률이 높아진다. 본 논문에서는 각 구간의 특징을 구분하기 위하여 해시값을 사용하였는데, 실험적으로 얻은 최적의 인증코드 길이는 16비트로서 이것의 우연에 의한 오탐지 확률은 $1/2^{16}$가지 즉, 1/65536 = 1.52588E-05의 확률이므로 그 가능성은 매우 낮

다고 할 수 있을 것이다. 구간의 인증코드로는 해시값 뿐만 아니라, 알고리즘을 적용할 응용에 따라 사용자에 특화된 고유ID/비밀번호/기관코드/장치ID/타임코드/비밀키 등을 응용목적에 따라 유연하게 사용할 수 있으며, 정확도를 높이기 위하여 인증코드의 길이를 더 길게 사용할 수도 있다.

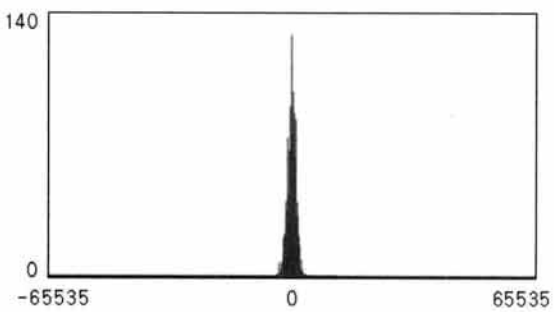
3. 가역 워터마킹 기반 인증정보 삽입 및 검출

히스토그램 쉬프팅 기법을 이용하는 가역 워터마킹 알고리즘들은 데이터를 삽입하려는 최대점 주위의 샘플링값 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 3(a))와 같이 일반적인 오디오 파형을 보면 진폭의 차이가 심하게 보이지만, (그림 3(b))처럼 확대하여 살펴보면 값들의 지역성이 높음을 알 수 있다. (그림 4)에 임의의 0.1초 구간에 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.



(그림 3) 오디오 파형(x축:시간, y축:음압):
(a)확대 전, (b)확대 후

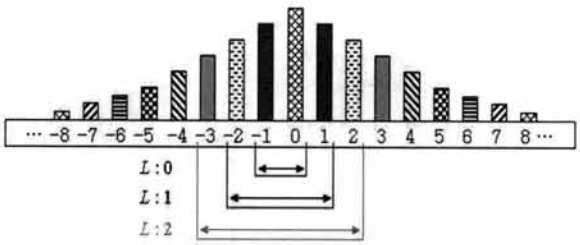


(그림 4) 0.1초 길이 구간에 대한 차이값
히스토그램(x축:차이값, y축:빈도수)

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.

본 논문에서는 각 구간 단위로 인증정보를 삽입 및 검출하기 위하여, 영상 콘텐츠 인증을 위하여 개발된 Yeo et al.[16] 연구의 차이값 히스토그램 기반 가역 워터마킹 알고리즘을 변형하여 사용하였다.

메시지는 차이값 히스토그램을 수정하여 삽입하게 되며, 삽입되는 메시지의 용량은 응용분야의 요구에 따라 삽입레벨 L로 조절한다. 0부터 시작되는 L 값에 따라 차이값 히스토그램에서 메시지 삽입에 이용되는 빈은 0번 빈 주위인 $\{(-L-1)\sim(+L)\}$까지로서 (그림 5)에 나타내었다. 본 논문에서 삽입해야할 구간별 인증코드의 길이는 16 비트이므로 구간의 삽입가능 용량이 충분한지 확인하여야 한다. 따라서 L의 값을 0부터 1씩 증가시키며 삽입가능한 용량을 확인하여 인증정보를 삽입할 수 있는 삽입레벨을 알아낸 후, 각 구간별로 인증코드를 삽입한다.



(그림 5) 메시지 삽입에 이용되는 히스토그램 빈

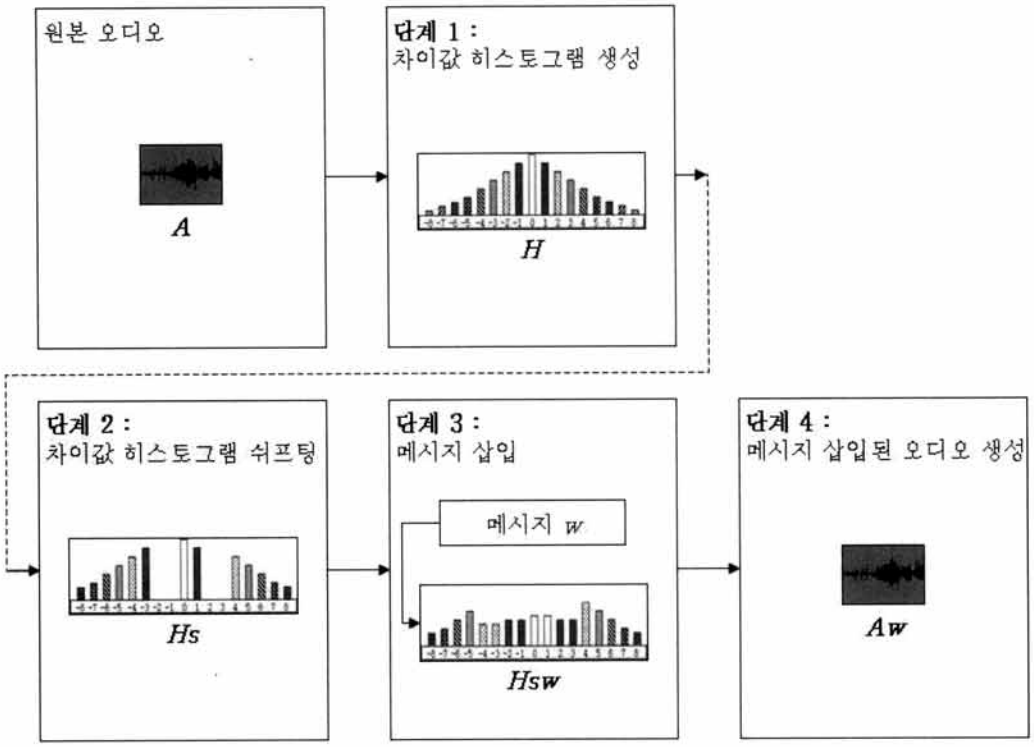
3.1 구간별 워터마크 삽입

(그림 6)은 각 구간에 대한 삽입 과정을 도시하였으며, 다음 4 단계의 과정을 거치게 된다. 삽입레벨 L=1일 때 각 단계의 예를 (그림 7)부터 (그림 9)까지에 나타내었다.

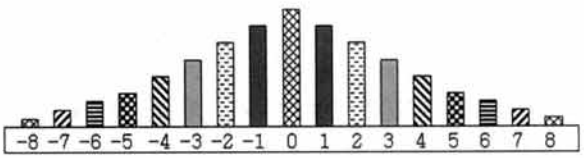
단계 1 : 오디오 A에 대하여 차이값 벡터 D를 구한다. 벡터의 첫 값은 오디오의 첫 샘플값으로 설정되고, 이후는 바로 앞 샘플과의 차이값으로 구성된다.

$$D_{(i)} = \begin{cases} A_{(0)}, & \text{if } i = 0 \\ A_{(i)} - A_{(i-1)}, & \text{otherwise} \end{cases} \quad \text{for } 0 \le i \le (sizeof(A) - 1). \tag{1}$$

단계 2 : 차이값 벡터로부터 차이값 히스토그램 H를 구한다음, 메시지 삽입을 위한 공간을 마련하기 위해 삽입레벨에 따라 다음과 같이 히스토그램을 쉬프트시킨다.



(그림 6) 각 구간에 대한 워터마크 삽입 절차

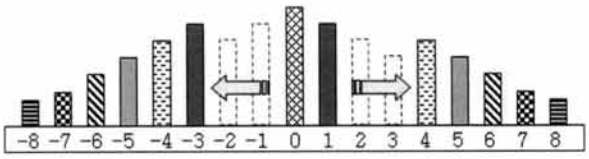


(그림 7) 삽입과정 단계 1 : 차이값 히스토그램 생성

$$Hs=\begin{cases}H+(L+1), & \text{if } H\geq(L+1)\\ H-(L+1), & \text{if } H\leq -1\end{cases} \quad (2)$$

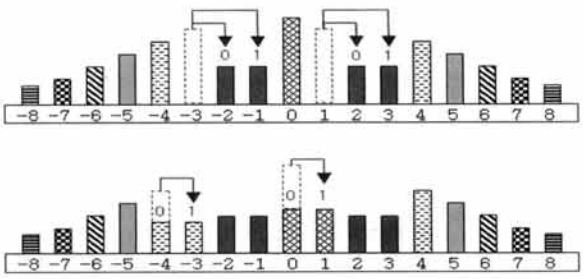
히스토그램 쉬프팅은 식 (3)과 같이 차이값 벡터를 수정하여 이루어진다.

$$Ds_{(i)}=\begin{cases}D_{(0)}, & \text{if } i=0\\ D_{(i)}+(L+1), & \text{if } D_{(i)}\geq(L+1)\\ D_{(i)}-(L+1), & \text{if } D_{(i)}\leq -1\end{cases} \quad (3)$$
$$\text{for } 0\leq i\leq(sizeof(A)-1).$$



(그림 8) 삽입과정 단계 2 : 차이값 히스토그램 쉬프팅

단계 3 : 히스토그램을 수정하여 메시지 $w(n)$를 삽입하는 과정은 다음 식 (4)와 같이 차이값 벡터를 수정하여 이루어진다.



(그림 9) 삽입과정 단계 3 : 메시지 삽입(4)

$$Dsw_{(i)}=\begin{cases}Ds_{(0)}, & \text{if } i=0\\ 2Ds_{(i)}+2L+2, & \text{if } -2L-2\leq Ds_{(i)}\leq -L-2 \text{ and } w(n)=0\\ 2Ds_{(i)}+2L+3, & \text{if } -2L-2\leq Ds_{(i)}\leq -L-2 \text{ and } w(n)=1\\ 2Ds_{(i)}, & \text{if } 0\leq Ds_{(i)}\leq L \text{ and } w(n)=0\\ 2Ds_{(i)}+1, & \text{if } 0\leq Ds_{(i)}\leq L \text{ and } w(n)=1\end{cases} \quad (4)$$
$$\text{for } 0\leq i\leq(sizeof(A)-1), \text{ where } w(n)\in\{0,1\}.$$

단계 4 : 메시지가 삽입된 수정된 히스토그램으로부터 메시지가 삽입된 최종 오디오를 구하는 절차는 다음 식 (5)를 통하여 이루어진다.

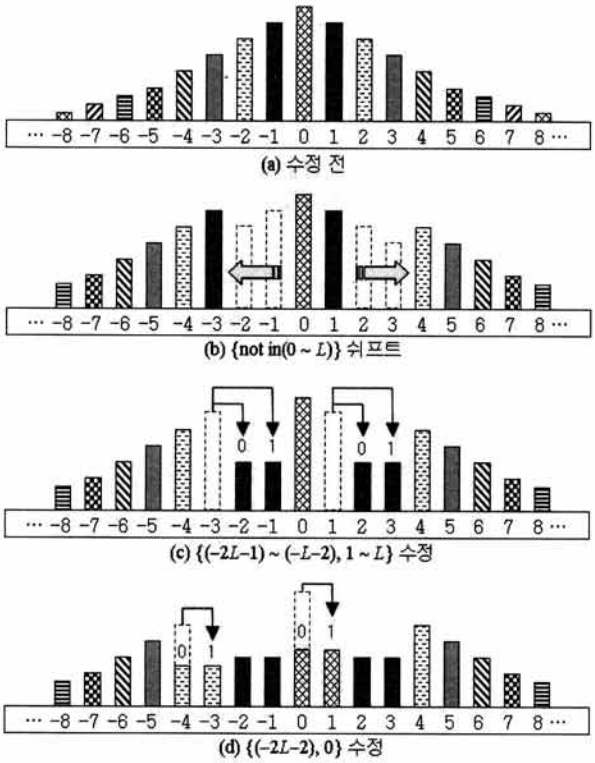
$$Aw_{(i)} = \begin{cases} Dsw_{(0)}, & \text{if } i = 0 \\ A_{(i-1)} + Dsw_{(i)}, & \text{otherwise} \end{cases} \quad \text{for } 0 \le i \le (sizeof(A) - 1). \tag{5}$$

차이값 벡터는 메시지가 삽입되어 쉬프트가 되어있는 상태이기 때문에 차이값 벡터만을 이용하여 오디오를 만들게 되면 앞 샘플들의 쉬프트된 누적분의 영향으로 올바른 오디오를 얻을 수 없음을 주의해야 한다.

삽입레벨 L이 1인 경우 메시지가 삽입되는 과정에서 히스토그램이 수정되는 절차를 (그림 10)에 나타내었다. 설명을 위해 (그림 10(c))와 (그림 10(d))는 각각 별도로 나타내었지만, 한 번의 차이값 벡터 스캔 과정을 거치며 수행된다.

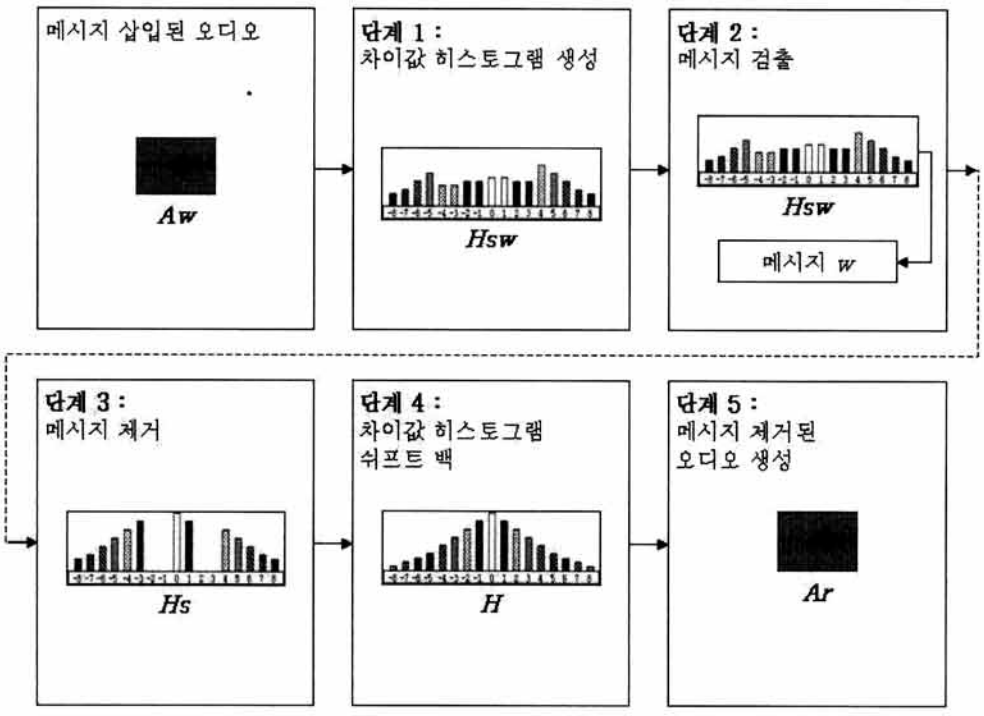
3.2 구간별 워터마크 검출 및 복원

워터마킹된 메시지를 검출하기 위해서는 삽입과정을 역순으로 진행하면 되는데, 다음 5 단계의 과정을 거쳐 원본 오디오를 복원하게 된다. 차이값 히스토그램의 특성상 샘플값을 복원하기 위해서는 앞 샘플값뿐만 아니라 앞 샘플과의 차이값 또한 같이 복원해야하므로, 복원 과정은 하나의 단계씩 완료되는 것이 아니라 1~5 단계의 과정을 한 샘플씩 반복하며 수행해야 한다. 전체 검출 및 복원 과정을 (그림 11)에 도시하였으며, 삽입레벨 L=1일 때 각 단계의 예를 (그림 12)부터 (그림 15)까지에 나타내었다.



(그림 10) 인증코드 삽입과정에서의 히스토그램 수정 절차 (삽입레벨 L=1의 경우)

단계 1 : 차이값 벡터를 다음 수식 (6)을 통하여 구한다. 복원된 오디오인 Ar의 첫 번째 값을 의미하는 $Ar_{(0)}$는 삽입과정에서 수정되지 않은 샘플값인 $Aw_{(0)}$의 값으로 결정된다.

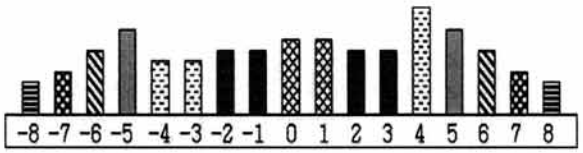


(그림 11) 각 구간에 대한 워터마크 검출 및 복원 절차

$$Dsw_{(i)} = \begin{cases} Aw_{(0)}, & \text{if } i=0 \\ Aw_{(i)} - Ar_{(i-1)}, & \text{otherwise} \end{cases} \quad \text{for } 0 \le i \le (sizeof(Ar)-1). \tag{6}$$

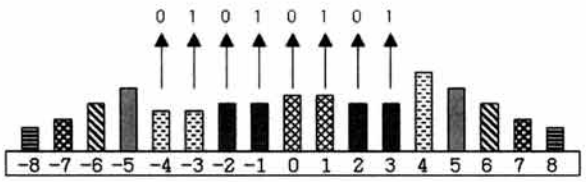
$$w(n) = \begin{cases} 0, & \text{if } -(2L+2) \le Dsw_{(i)} \le -1 \text{ and } \bmod(Dsw_{(i)}, 2) = 0 \\ 1, & \text{if } -(2L+2) \le Dsw_{(i)} \le -1 \text{ and } \bmod(Dsw_{(i)}, 2) = -1 \\ 0, & \text{if } 0 \le Dsw_{(i)} \le (2L+1) \text{ and } \bmod(Dsw_{(i)}, 2) = 0 \\ 1, & \text{if } 0 \le Dsw_{(i)} \le (2L+1) \text{ and } \bmod(Dsw_{(i)}, 2) = 1 \end{cases} \quad \text{for } 1 \le i \le (M \times N - 1). \tag{7}$$

$$Ds_{(i)} = \begin{cases} Dsw_{(0)}, & \text{if } i=0 \\ \left\lfloor \frac{Dsw_{(i)}}{2} \right\rfloor, & \text{if } 0 \le Dsw_{(i)} \le (2L+1) \\ \left\lfloor \frac{Dsw_{(i)} + (2L+2)}{2} \right\rfloor - (2L+2), & \text{if } -(2L+2) \le Dsw_{(i)} \le -1 \\ Dsw_{(i)}, & \text{otherwise} \end{cases} \quad \text{for } 0 \le i \le (sizeof(Ar)-1). \tag{8}$$



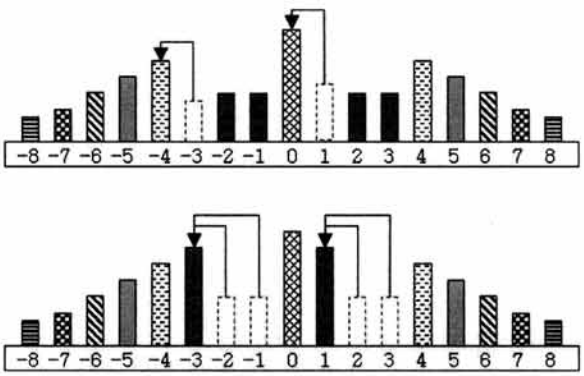
(그림 12) 복원과정 단계 1 : 차이값 히스토그램 생성

단계 2 : 계산된 차이값을 이용하여 삽입된 메시지를 검출한다. 메시지가 삽입된 공간이 아니면 다음 단계로 넘어간다.



(그림 13) 복원과정 단계 2 : 메시지 검출

단계 3 메시지를 제거한다. 메시지가 삽입된 공간이 아니면 다음 단계로 넘어간다.



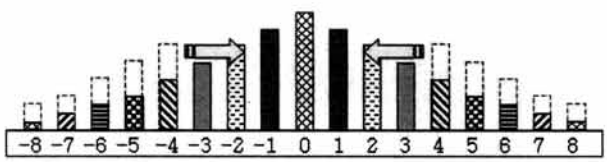
(그림 14) 복원과정 단계 3 : 메시지 제거

단계 4 : 메시지를 삽입하기 위한 공간을 마련하기 위하여 쉬프트하였던 차이값 히스토그램을 원위치로 복구시킨다.

$$H = \begin{cases} Hs - (L+1), & \text{if } Hs \ge (2L+2) \\ Hs + (L+1), & \text{if } Hs \le -1 \end{cases} \tag{9}$$

이 과정은 다음 식 (10)과 같이 차이값 벡터를 수정함으로써 수행된다.

$$D_{(i)} = \begin{cases} Ds_{(0)}, & \text{if } i=0 \\ Ds_{(i)} - (L+1), & \text{if } Ds_{(i)} \ge (2L+2) \\ Ds_{(i)} + (L+1), & \text{if } Ds_{(i)} \le -1 \\ Ds_{(i)}, & \text{otherwise} \end{cases} \quad \text{for } 0 \le i \le (sizeof(Ar)-1). \tag{10}$$



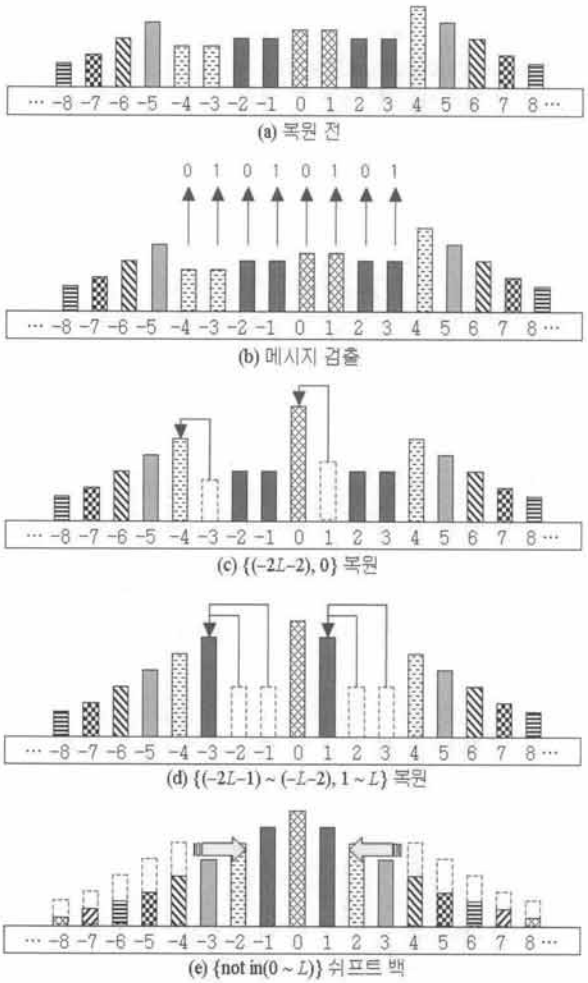
(그림 15) 복원과정 단계 4 : 차이값 히스토그램 쉬프트 백

단계 5 : 복원된 앞 샘플과 복원된 차이값을 이용하여 원 오디오를 복원한다.

$$Ar_{(i)} = \begin{cases} Aw_{(0)}, & \text{if } i=0 \\ Ar_{(i-1)} + D_{(i)}, & \text{otherwise} \end{cases} \quad \text{for } 0 \le i \le (sizeof(Ar)-1). \tag{11}$$

메시지를 복원하는 과정에서 히스토그램이 수정되는 과정을 (그림 16)에 나타내었다. 삽입할 때와 마찬가지로 (그림

16(c))와 (그림 16(d))는 이해를 돕기 위하여 각각 별도로 나타내었지만, 한 번의 차이값 벡터 스캔 과정을 거치며 수행된다.



(그림 16) 메시지 검출 및 복원과정에서의 히스토그램 수정 절차 (삽입레벨 $L=1$의 경우)

4. 실험 및 성능 평가

다양한 장르의 7곡을 선정하여 실험에 사용하였으며, 오디오 데이터 파일의 형식은 16KHz 샘플링레이트의 16bit 샘플 모노 PCM Wave이다. 정밀한 인증을 수행하기 위하여 0.1초 길이 구간 단위로 인증실험을 수행하였다. 인증정보가 삽입된 오디오 콘텐츠의 품질은 다음 식 (12)의 SNR (The signal-to-noise ratio) 측정방식을 이용하였다. x(n)은 원본 오디오 콘텐츠 이며, x'(n)은 워터마킹된 오디오 콘텐츠이다.

$$SNR = 10 \cdot \log_{10} \frac{\sum_{\forall n} (x_{(n)})^2}{\sum_{\forall n} (x_{(n)} - x'_{(n)})^2} \qquad (12)$$

워터마킹된 오디오 콘텐츠에 대하여 볼륨 조절 및 에코 추가 공격을 가하고, 인증 확인을 수행한 결과를 <표 1>에 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 구간에 대하여 위변조를 탐지할 수 있었다. 만일, 인접 샘플간의 지역성이 높지 않아서 차이값의 변화가 큰 일부 오디오의 경우라면 필요한 삽입공간을 확보하기 위하여 삽입레벨을 높이게 된다.

오디오 워터마킹에 대한 기존 연구들은 대부분 강인성 워터마킹이지만, 본 논문에서 제안한 알고리즘은 연성 워터마킹이므로 미미한 공격에도 쉽게 워터마크로 삽입한 인증정보가 손상되어야 한다. 실험을 통하여 확인한 바와 같이 샘플값의 작은 변화에도 인증정보가 손상되므로, 콘텐츠의 무결성을 확인하는 용도로 이용되어 질 수 있다. 실험에 사용하지 않은 TSM, FSM, 피치 쉬프팅, 잘라내기 등의 공격도

〈표 1〉 오디오 워터마킹 및 인증 실험결과

오디오	오디오 내용	삽입레벨	SNR(dB)	인증률(%)
Clip01	이선희 "떠나지마"	0	83.51	100.0
Clip02	Mariah Carey "Without You"	0	83.34	100.0
Clip03	Mariah Carey "My All"	0	83.66	99.7
Clip04	Numeriklab "Ncis Theme Song"	0	87.87	99.3
Clip05	Bob Dylan "Things Have Changed"	0	84.59	100.0
Clip06	John Mellencamp "Troubled Land"	0	87.08	100.0
Clip07	"YTN 뉴스채널" 뉴스 녹음	0	82.97	99.6
평균	-	0	84.72	99.8

샘플값의 변화를 가져오므로 위변조를 인증할 수 있다. 또한 기존 연구들은 인증의 용도보다는 기밀정보를 강인하게 삽입하는 것이 주목적이다. 따라서 인증코드를 강인하게 삽입하여 인증에 사용할 수도 있겠지만 구간별 인증이 아닌 전체 오디오에 대한 한 번의 인증만 가능하다. 본 논문에서 제안하는 방법은 구간별 인증이 가능할 뿐만 아니라, 하나의 구간이라도 위변조를 탐지하였다면 전체 오디오에 대한 한 번의 인증이 가능하므로 더욱 정확한 인증률을 얻을 수 있다.

스테레오 오디오인 경우는 각 채널별로 동일한 알고리즘을 적용하여 더욱 정밀한 인증을 수행할 수 있다. 또한 주파수 변환 영역이 아닌 단순 산술 연산으로 인증이 가능하므로 계산능력이 제한적인 임베디드 장치등에도 적용할 수 있다.

5. 결론 및 향후 연구방향

본 논문에서는 오디오 콘텐츠의 무결성을 검증하기 위한 알고리즘으로서, 원본 오디오를 구간 단위로 분할하여 각 구간에 인증정보를 삽입함으로써 공격자에 의한 손상여부를 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.

참 고 문 헌

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography," Morgan Kaufmann Publishers Inc., San Francisco, CA, 2007.

[2] J. Fridrich, J. Goljan and R. Du, "Invertible authentication," Proc. of the SPIE, Security and Watermarking of Multimedia Contents, San Jose, CA, Vol.4314, pp.197-208, Jan., 2001.

[3] F. Mintzer, J. Lotspiech and N. Morimoto, "Safeguarding digital library contents and users: digital watermarking," D-Lib Magazine, Dec., 1997.

[4] S. Katzenbeisser and F. A. P. Peticolas, Eds., Information Hiding Techniques for Steganography and Digital Watermarking. Norwell, MA: Artech House, 2000.

[5] H. T. Sencar, M. Ramkumar, A. N. Akansu, and A. Sukerkar, "Improved utilization of embedding distortion in scalar quantization based data hiding techniques," EURASIP Signal Process. J. (Elsevier), Vol.87, pp.877 - 890, May, 2007.

[6] J. Haitsma, T. Kalker, and F. Bruekers, "Audio watermarking for monitoring and copy protection," in Proc. 8th ACM Multimedia Workshop, Los Angeles, CA, pp.119 - 122, 2000.

[7] D. Kirovski and H. S. Malvar, "Spread-spectrum watermarking of audio signals," IEEE Trans. Signal Process., Vol.51, No.4, pp.1020 - 1033, Apr., 2003.

[8] R. Tachibana, S. Shimizu, T. Nakamura, and S. Kobayashi, "An audio watermarking method robust against time- and frequency-fluctuation,"in Proc. SPIE Security and Watermarking of Multimedia Contents III, San Jose, CA, Vol.4314, pp.104 - 115, 2001.

[9] R. Tachibana, "Improving audio watermark robustness using stretched patterns against geometric distortion," Proc. PCM Adv. Multimedia Inf. Process., Vol.2532, pp.647 - 654, 2002.

[10] M. Mansour and A. Tewfik, "Audio watermarking by time-scale modification,"in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, Vol.3, pp.1353 - 1356, May, 2001.

[11] M. Mansour and A. Tewfik, "Data embedding in audio using time-scale modification," IEEE Trans. Speech Audio Process., Vol.13, No.3, pp.432 - 440, May, 2005.

[12] W. Li, X. Xue, and P. Lu, "Localized audio watermarking technique robust against time-scale modification," IEEE Trans. Multimedia, Vol.8, No.1, pp.60 - 69, Feb., 2006.

[13] S. Xiang and J. Huang, "Histogram-based audio watermarking against time-scale modifications and cropping attacks," IEEE Trans. Multimedia, Vol.9, No.7, pp.1357 - 1372, Nov., 2007.

[14] X. Zhang, D. Chang, W. Yang, Q. Huang, W. Guo and Y. Zhao, "An Audio Digital Watermarking Algorithm Transmitted via Air Channel in Double DCT Domain," 2011 International Conference on Multimedia Technology (ICMT), pp.2926-2930, Jul., 2011.

[15] X. Huang, I. Echizen, and A. Nishimura, "A new approach of reversible acoustic steganography for tampering detection," Proc. of Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2010), pp.538 - 542, Nov., 2010.

[16] 여동규, 이해연, "차이값 히스토그램 기반 가역 워터마킹을 이용한 블록 단위 영상 인증 알고리즘", 정보처리학회논문지 Vol.18B, No.6, Dec., 2011.

여 동 규

e-mail : sylot@kumoh.ac.kr

1999년 국립금오공과대학교 컴퓨터공학과 (학사)

2001년 국립금오공과대학교 컴퓨터공학과 (공학석사)

2010년 국립금오공과대학교 컴퓨터공학과 (공학박사)

2010년~현 재 국립금오공과대학교 모바일연구소 박사후연구원

관심분야 : 정보보호, 디지털워터마킹, 디지털포렌식 등

이 해 연

e-mail : haeyeoun.lee@kumoh.ac.kr

1997년 성균관대학교 정보공학과(학사)

1999년 한국과학기술원 전산학과(공학석사)

2006년 한국과학기술원 전자전산학과 전산학전공(공학박사)

2001년~2006년 (주)쎄트렉아이 선임연구원

2006년~2007년 코넬대학교 박사후연구원

2008년~현 재 국립금오공과대학교 컴퓨터공학부 교수

관심분야 : 멀티미디어, 영상처리, 콘텐츠보안, 디지털워터마킹 등