논문-01-6-3-07

블라인드 워터마킹: 튜토리얼

김 형 중*, 여 인 권*

Blind Watermarking Algorithms: A Tutorial

Hyoung-Joong Kim* and In-Kwon Yeo*

요 약

이 논문은 현재 잘 알려진 3종류의 블라인드 워터마크 삽입 및 검출방법을 신호처리 관점에서 소개한다. 이들 3가지는 각각 상관관계기반 방법, 에코기반 방법, 그리고 패치워크 방법이다. 이들 방법은 시간영역 (또는 공간영역) 또는 변환영역에서 적용할 수 있다. 이 논문에서는 이들 세 방법을 구현하는데 필요한 기초이론 및 구현방법을 제공한다. 아울러 실제 약간의 실험 결과들을 포함시켰다.

Abstract

This paper introduces three well-known blind watermarking algorithms in terms of signal processing aspects. Those three methods include correlation-based, echo-hiding, and patchwork algorithms. Those algorithms can be applied either in time-domain (or equivalently spatial-domain) or frequency-domain (or equivalently transform-domain). This paper describes watermark embedding and detection algorithms as well as basic ideas for those watermarking algorithms. In addition, we include some experimental results.

Ⅰ. 워터마크 개론

디지털 워터마크라는 용어가 사용된 것은 최근의 일이지만 워터마크라는 용어는 오래 전부터 사용되었다. 예를 들면 해도의 수위를 나타내는 등고선 같은 선을 워터마크라고 불렀다. 또 빛에 비추어야만 보이는 지폐 속의 그림도 워터마크라고 부른다. 복사기로는 지폐의 워터마크를 복사할 수 없기 때문에 불법복제를 방지할 수 있다. 지폐에서의 워터마크 개념을 빌려와 디지털 컨텐츠의 불법복제를 방지하기 위해 디지털 워터마크라는 용어가 만들어졌고 역시 비슷하게 복제방지 목적으로 이용하기 시작했다.

* 강원대학교 제어계측공학과
Department of Control and Instrumentation Engineering, Kangwon National University

오늘날 우리가 신호처리에서 사용하는 의미의 워터마크라는 용어가 처음 등장한 것은 1993년이다. Tirkel과 그의 동료들이 "워터 마크"라는 두 단어를 처음 사용한 것이 시발점이었다[10]. 그 이후 워터마크는 디지털 데이터를 보호하기 위한 중요한 기술 가운데 하나로 자리잡게 되었다. 워터마크는 디지털 데이터 신호에 숨기는 특별한 정보 또는 데이터를 말한다. 워터마크는 눈에 보이는 워터마크, 귀에 들리는 워터마크도 있지만 일반적으로는 보이지 않고 들리지도 않는 워터마크가 주로 이용된다. 워터마크는 비즈니스 모델에 따라 종류가 다양하다. 전자도서의 지적재산권을 보호하기 위해 문장 속에 숨기는 텍스트 워터마크도 있다. 또 반도체 회로의 지적재산권을 보호하기 위해 회로나 회로 안에서 생성되는 신호 속에 워터마크를 숨기기도 한다. 그렇지만 이 논문에서는 특별히 비디오 워터마크와 오디오 워터마크만 다룬다.

1. 신호처리 영역

워터마크는 디지털 신호처리 기술에 크게 의존한다. 워터마크가 숨겨진 신호, 즉 사본신호 $s[k]$는 신호성분 $x[k]$와 워터마크 신호 $w[k]$의 함수로 표현된다. 즉,

$$s[k] = f\{x[k], w[k]\} \tag{1}$$

로 표시한다. 오디오는 1차원 신호, 즉 시간의 함수로만 표현되므로 $s[k]$와 같이 표현하는 것이 자연스럽다. 그리고 그것이 시간 k의 함수이기 때문에 시간영역에서의 표현이라고 부른다. 우리가 다루는 영상은 2차원 영상으로 직각좌표계에서는 $s(x, y)$로 표현한다. 그리고 2차원부터는 시간영역이라고 부르는 대신 공간영역이라고 부른다. 영상 프레임 하나 하나가 특정한 시간 k에서 얻은 것이고 그 순간에 얻은 영상은 좌표 x와 y에서의 픽셀 값들로 구성되어 있다. 그러나 특별한 구분을 하지 않을 때는 1차원이나 2차원 모두 편의상 $s[k]$와 같이 표현하며, 시간영역이나 공간영역도 구분하지 않고 혼용해서 사용하기로 한다.

시간영역이나 공간영역에 대응되는 용어가 변환영역이다. 시간영역의 정보를 DFT 변환해서 주파수영역으로 옮기면 시간영역에서 얻을 수 없는 결과를 확보할 수 있다. 모든 변환이 다 주파수영역으로 옮겨주는 것은 아니므로 변환영역이라고 부른다. 여기서도 변환영역이나 주파수영역을 혼용하기로 한다.

워터마크는 시간영역과 공간영역 어디서나 삽입할 수 있다. 그러나 그 성질은 많이 다르다. 시간영역에서 삽입한 워터마크는 공격에 약하다. 그렇지만 시간영역에서 워터마크를 삽입하는 것은 변환이 필요하지 않기 때문에 구현이 비교적 간단하다. 그러나 주파수영역에서 워터마크를삽입할 때는 그림 1과 같은 변환이 필요하다. 이때 흔히 사용하는 변환방법으로는 DCT, DFT, DWT가 있다. 그래서 두 영역의 방법들을 적절히 혼용하는 것이 바람직하다.

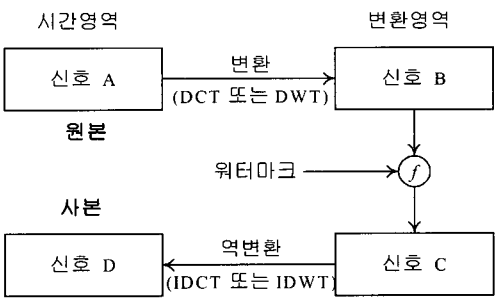

그림 1. 변환영역에서의 워터마크 삽입과정
Fig. 1. Watermark embedding process in the transform-domain

2. 신호처리기술 대 통신기술

최근에는 워터마킹에 통신에서 개발된 다양한 기술을 원용하려는 움직임도 일고 있다. 통신기술의 역사가 오래되어 많은 연구결과가 축적되어있기 때문에 워터마킹 연구에 참고할만한 것이 많다. 물론 통신과 디지털신호처리에서 보는 신호나 잡음에 대한 관점의 차이는 어느 정도 존재한다. 통신에서는 큰 신호 $x[k]$에 작은 잡음 $w[k]$가 포함되는 것을 전제로 한다. 이때 $s[k]$에서 원래의 신호 $x[k]$를 가능하다면 원상대로 복원하기 위해 잡음 $w[k]$를 효과적으로 제거하거나 그 영향을 최소화하는 것이 통신에서의 목표이다. 통신에서 잡음 $w[k]$는 전혀 원치 않는 신호이며, 잡음 $w[k]$의 성질도 대부분 미리 알 수 없기 때문에 잡음을 처리할 때 많은 어려움을 겪는다.

한편 워터마크에서는 잡음에 해당하는 $w[k]$를 사실상 고의로 집어넣는다. 그리고 그 잡음성분에 해당하는 $w[k]$는 알고있는 신호이다. 오히려 신호성분인 $x[k]$가 예측하기 어려운 신호일 경우가 많다. 그래서 워터마크에서는 $w[k]$를 잡음이라 부르지만 사실은 $w[k]$가 신호에 해당하고 성질을 잘 모르는 $x[k]$가 잡음에 해당한다. 그러나 혼란을 피하기 위해 $x[k]$를 신호로, $w[k]$를 잡음으로 부르기로 한다.

결론적으로 통신과 신호처리 측면에서 두 기술 사이에는 다른 점도 있지만 비슷한 점도 많아 통신기술도 워터마크 기술에 유용하게 응용될 수 있다.

3. 확산대역 기술

통신기술이 달성한 놀라운 업적 가운데 하나가 확산대역 기술이다. 이 기술의 핵심은 스펙트럼을 확산시켜 스펙트럼 검출을 어렵게 하자는 것이다[3]. 검출이 어려워지면 통신비밀은 더 강화된다. 당연히 워터마크에서도 공격에 잘 견디도록 확산대역 기술을 사용하여 비밀을 유지하기 위한 용도로 응용할 수 있다. 확산대역 기법은 시간영역에서의 확산과 주파수영역에서의 확산으로 구분할 수 있다. 시간영역에서 변화속도가 느린 신호는 그림 2(a)처럼 스펙트럼 높이가 높고 그곳에 에너지가 집중되는 현상을 보

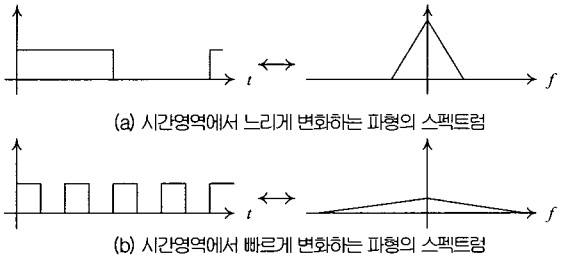

그림 2. 시간영역에서의 신호 변화에 대응하는 스펙트럼 분포도
Fig. 2. Spectrums of signals in time-domain

여준다. 그러나 시간영역에서 빨리 변화하는 신호의 스펙트럼은 그림 2(b)처럼 넓은 영역에 걸쳐 확산되는 것을 확인할 수 있다. 스펙트럼이 낮고 넓은 범위에 걸쳐 나타나므로 검출이 상대적으로 더 어렵게 된다. 왼편 구형파의 스펙트럼은 sinc(f)로 표현해야 하나, 편의상 삼각파로 나타냈다.

그리고 시간영역에서 그림 2(a)의 왼편처럼 신호가 천천히 변하면 신호 값을 예측하기 쉽다. 따라서 신호를 그림 2(b)와 같이 빨리 변하도록 할 필요가 있다. 한편 그림 2(b)와 같이 빨리 변화하는 신호는 저역필터를 통과시키면 신호의 특성이 많이 사라져버리는 단점이 있다. 이런 점이 공간영역에서 워터마크를 삽입할 때 흔히 부딪히는 문제이다. 그래서 대신 그림 2(a)의 오른편 스펙트럼에 워터마크를 삽입하고 그것을 다시 역변환해두면 시간영역에서는 잡음이 전 영역에 고루 확산되므로 주파수 공격에 잘 견디게 된다. 그렇지만 스펙트럼의 어떤 영역에 워터마크를 삽입하는 것이 좋은지에 대해서는 깊이 생각해야 한다.

4. 블라인드 워터마크

원본이 있어야 워터마크 검출이 가능한 것과 원본이 없어도 워터마크 검출이 가능한 두 종류의 워터마크가 있다. 후자를 블라인드 워터마크라고 부른다. 그림 3은 원본이 불필요한 블라인드 워터마크 방식을 도식적으로 보여준다. 검출과정에서 원본신호 $x[k]$가 전혀 사용되고 있지 않다. 공격에 의해 잡음 $n[k]$가 추가되어 워터마크 검출이 더 어려워지지만 여전히 $x[k]$없이도 $w[k]$의 검출이 가능하다.

그렇다면 블라인드 워터마킹이 가지고 있는 장점은 무엇인지 알 필요가 있다. 그 이유는 다음과 같다. (단, 워터마크는 $s[k] = x[k] + w[k]$ 방식을 쓴다고 가정한다.)

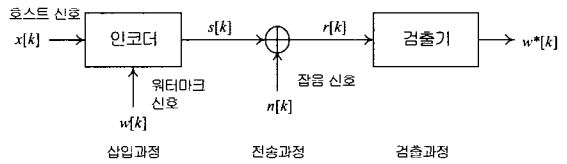

그림 3. 블라인드 워터마크 삽입과 검출 과정
Fig. 3. Embedding and detection of blind watermark

1) 워터마크를 찾기 위해 원본과 사본이 동시에 필요하다면 둘을 동시에 저장하고 전송해야 하므로 저장공간의 낭비 및 통신 대역의 낭비를 초래하게 된다.
2) 공격을 받지 않았을 때만 $w[k] \approx s[k] - x[k]$가 될 수 있다. 공격 받으면 $r[k] - x[k] \approx w[k] + n[k]$가 되어 워터마크 검출이 어렵다. 결국 $x[k]$의 유무가 워터마크 검출에 영향을 미치지 않을 수 있다.
3) 검출에 원본이 필요하다면 원본에 접근하는 문제가 있다. 누군가가 원본을 훼손시킬 가능성이 있기 때문이다. 그러므로 원본이라는 것을 누구나 인정할 수 있는 여건이 형성되어야 한다. 아무나 자기 것이 원본이라고 주장할 수도 있기 때문이다. 그리고 원본이 없을 때 소유권 주장에 더 설득력이 있다는 보고가 있다[4].
4) 원본이 없을 때 더 효율적인 응용분야가 많이 있다. 예를 들면 웹 로봇이 웹사이트를 검색하며 불법 복제물이 있는지를 검사하고 있다고 가정하자. 이때 대량의 복제물에 대해 일일이 원본과 비교하는 것은 현실적으로 불가능하다.
5) 공격하면서 사본의 크기를 줄이거나 늘이며 변형시키면 원본이 있어도 둘 사이의 차이를 구하는 것이 현실적으로 불가능하고, 차이를 구한다고 해도 의미를 부여하기 어렵다.

5. 블라인드 워터마크 종류

현재까지 알려진 방법으로 블라인드 워터마크 기법은 크게 네 종류로 나눌 수 있다. 이들은 상관관계기반 방법[2][3][4][6][7][9], 에코기반 방법[2][13], 패치워크 방법[1][2][8][12] 그리고 양자화 방법[5] 등이다. 이들 방법은 시간영역 (또는 공간영역) 또는 변환영역에서 적용할 수 있다. 이들을 정리하면 그림 4와 같다. 그림 4에서 분류한 바에 의하면 상관관계 기반 방식은 워터마크를 삽입할 때

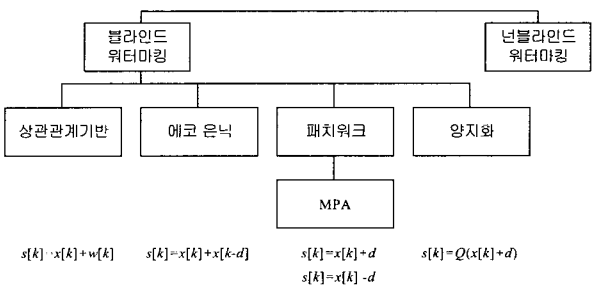

그림 4. 블라인드 워터마크의 분류
Fig. 4. Classification of watermarking algorithms

$$s[k] = x[k] + \alpha \cdot w[k] \quad (2)$$

와 같이 워터마크 잡음 $w[k]$와 신호성분 $x[k]$를 더한다. 반대로 워터마크를 검출할 때는 $w[k]$와 $x[k]$의 상관관계를 구한다. 그래서 이 방법을 상관관계 방법이라고 부른다. 에코 기반 방법은

$$s[k] = x[k] + \alpha \cdot x[k-d] \quad (3)$$

와 같이 원래 신호 $x[k]$에 에코 성분 $x[k-d]$를 더한다. 여기서 워터마크 정보는 d가 된다. 패치워크 방법은 통계적 성질이 비슷한 두 집합을 선정해 한 샘플 집합 A의 원소들은 $x[k]$에 d를 더하고 다른 집합 B에서는 d를 뺀다. 즉

$$s_A[k] = x[k] + d \quad (4)$$

$$s_B[k] = x[k] - d \quad (5)$$

가 되도록 만든다. 워터마크를 검출할 때는 $E\{s_A[k] - s_A[k]\} = 2d$가 될 것이라는 가정 아래 통계적 기술을 적용한다. 양자화 방법에서는 $x[k]$에 d를 더한 후 양자기 Q를 써서 정보를 변형한다. 그렇지만 워터마크를 검출할 때는 역시 상관관계를 계산하기 때문에 사실 상관관계 기반 방법과 매우 유사하다.

Ⅱ. LBM (Least-Significant Bit Modulation)

초기의 워터마킹 기법은 매우 단순해서 이해하기 쉬웠지만 그만큼 공격에도 쉽게 무너지는 약점을 지니고 있었다. 이런 워터마크의 기본 개념은 원본신호 $x[k]$의 LSB (Least-Significant Bit) 값을 바꾸는 것이었다. LSB를 선택한 것은 그 값이 신호 $x[k]$에 가장 적게 영향을 미쳤기 때문이다. 만일 공격을 받지않았다면 당연히 $s[k]$로부터 쉽게 $w[k]$를 검출할 수 있다. 지금 거의 이 방법을 쓰지 않는 가장 큰 이유는 공격에 매우 약하다는 점이다. 일단 모든 LSB의 값을 임의로 불규칙하게 바꿔버리면 워터마크가 사라져버린다. 또 고역필터나 저역필터를 통과시키면 숨긴 잡음이 쉽게 제거될 수 있다는 문제점을 지니고 있다.

LSB를 고쳤기 때문에 앞서 가정했던 것처럼 당연히 신호에 미치는 영향은 그리 크지 않다고 가정할 수 있다. 그렇지만 오디오신호에서 LSB를 바꾸더라도 귀에 잡음으로 들리는 경우가 많다. 작은 소리에 귀가 더 민감하고 큰 소리에는 상대적으로 둔감하다. 그런데 소리가 작을 때는 LSB를 바꾸는 것만으로도 귀에 쉽게 감지될 수 있다. 그렇지만 귀가 눈에 비해 더 민감하기 때문에 오디오에서는 작은 워터마크 신호도 분명한 잡음이 될 수 있지만 이미지나 비디오에서는 눈으로 그 차이를 식별하기 어려울 때가 많다.

1. 워터마크신호 $w[k]$의 성질

워터마크신호 $w[k]$는 원본신호 $x[k]$를 훼손시킨다. 따라서 $w[k]$는 잡음이라고 볼 수도 있다. 한편 워터마크는 비록 잡음일지라도 $w[k]$는 신호의 품질과 워터마크 본연의 목적에 맞추어 만들어진 규칙들을 지켜야 한다. 그런 것들을 정리하면 다음과 같다.

1) 삽입할 워터마크 신호 $w[k]$는 난수의 성질을 지녀야 한다. 난수처럼 불규칙해서 공격자들이 $w[k]$를 예측하기 어렵게 만들어야 한다. 그렇지 않으면 공격자들이 쉽게 신호 $w[k]$를 유추한다.
2) 난수는 다시 원래대로 재생이 가능해야 한다. 이런 성질을 만족하는 난수를 유사난수 (Pseudo-random Noise) 또는 PN 시퀀스라고 부른다. 유사난수를 써야 삽입기가 사용한 것과 동일한 유사난수를 검출기에서도 재생할 수 있고, 그것을 써서 워터마크를 복원할 수 있다.
3) 잡음이 -1과 1 사이의 수로 표현될 경우 평균은 0에 가까운 것이 좋다. 만일 1이나 -1에 가까운 쪽으로 편이 (Bias) 현상이 생기면 공격자 입장에서 난수의 유추 가능성이 높아지며, 직류성분이 증가하게 되어 검출특성을 저하시킨다.

2. 잡음 $w[k]$의 삽입

원본신호 $x[k]$에 워터마크신호 $w[k]$를 첨가하는 방법은 크게 가산형과 승산형으로 나눈다. 가산형이란 $x[k]$와 $w[k]$를 더하는 형태로, 식으로 표시하면 다음과 같다.

$$s[k] = x[k] + \alpha w[k] \quad (6)$$

여기서 α는 잡음의 강도를 나타낸다. 이 방법은 신호의 크기에 무관하게 워터마크 신호가 결정되므로 큰 신호에는 작은 워터마크 신호가 되거나 작은 신호에는 큰 워터마크 신호가 될 수 있다. 따라서 신호의 특성에 무관하게 되는 단점이 있다. 또 디지털신호 시스템 숫자

표현에서 오버플로우나 언더플로우 현상을 초래하기도 한다. 예를 들어 [0, 255] 사이의 신호 가운데 255에 1만 더해도 256이 되면서 문제를 일으킬 수 있다. 마찬가지로 0에 대해 1을 빼도 역시 [0, 255] 범위를 벗어나 문제가 된다.

승산형 잡음삽입은 $x[k]$와 $w[k]$를 곱하는 형태로 식으로 표시하면 다음과 같다.

$$s[k] = x[k]\{[1 + \alpha w[k]\} \quad (7)$$

승산형은 신호의 특성에 따라 큰 값은 더 크게, 작은 값은 더 작게 만드는 효과가 있다. 특별히 오디오에서 신호가 작을 때 잡음도 작아지므로 잡음이 잘 들리지 않게 된다. 한편 신호가 클 때는 큰 잡음이 첨가되더라도 일종의 마스킹 (Masking) 효과에 의해 잡음이 잘 들리지 않게 된다. 그리고 이때의 큰 잡음은 워터마크의 강인성을 높여주는 효과가 있다.

3. 잡음 $x[k]$의 생성

잡음은 정수형 잡음과 실수형 잡음으로 구분할 수 있다. 정수형은 0과 1, 또는 -1과 1의 단 두 값만을 갖는 바이너리 잡음이 일반적으로 사용된다. 실수형 잡음은 -1과 1 사이의 모든 실수 값을 갖는다.

실수형 잡음은 난수발생기 출력을 쓰는데 일반적으로 확률분포가 균일분포 (Uniform Distribution) 특성을 갖는 것과 정규분포를 갖는 것을 주로 사용한다. 균일분포 잡음의 크기는 범위가 (예를 들면 -1에서 1까지) 제한되기 때문에 지나치게 큰 잡음이 발생하지 않아 가산형을 쓸 경우 잡음의 효과를 예측할 수 있고 오버플로우 현상을 어느 정도 예방할 수 있다. 이에 반해 정규분포 잡음에서는 매우 큰 잡음도 발생할 가능성이 (확률적으로 낮기는 하지만 조금이라도) 있기 때문에 잡음으로 삽입할 때 주의가 요구된다. 그러나 정규분포 잡음은 통계적 해석이 용이하다는 장점을 지니고 있다.

특히 잡음은 평균이 0이 되도록 할 필요가 있다. 상관관계 (Correlation) 특성을 이용해 워터마크 유사도를 측정하는 경우 잡음 평균이 0이 아니면 성능을 저하시키는 요인이 되기도 한다. 일반적으로 정규분포 잡음은 평균 0, 분산 1이므로 유사도 측정에서 문제를 일으키지 않는다. 그러나 균일분포 잡음은 평균이 0이 아니면 평균 0이 되도록 적절한 조처를 취해주어야 한다.

Ⅲ. 상관관계기반 확산대역 기법

앞에서 살펴본 바와 같이 확산대역 기법은 크게 두 가지로 분류할 수 있다. 하나는 시간영역에서 확산시키는 방법과 다른 하나는 변환영역에서 확산시키는 방법이다. 전자는 식 (6)이나 (7)과 같이 삽입하고 후자는 $S[n] = X[n] + \alpha W[n]$이나 $S[n] = X[n]\{[1 + \alpha W[n]\}$과 같이 주파수영역에서 확산시킨다. 전자와 같이 삽입하는 것은 Hartung과 Girod [6]의 방법이 대표적이며, 후자는 Cox 등 [3]의 방법이 대표적이다. 전자의 가장 원시적 형태가 앞에서 살펴본 LBM이다. 여기서는 확산대역 방법의 특성을 소개한다.

1. 유사도

삽입한 잡음이 검출한 잡음과 어느 정도 유사한지를 교차상관관계로 확인하는 방법도 있다. 그러나 보다 정량적으로 비교하기 위해 유사도 (Similarity) 척도를 사용하기도 한다[3]. 원래의 워터마크 $w[k]$와 추출한 워터마크신호 $w^*[k]$사이의 유사도는 다음과 같이 정의된다.

$$sim(w, w^*) = \frac{w^* \cdot w}{\sqrt{w^* \cdot w^*}} \quad (8)$$

여기서 $w[k]$와 추출된 $w^*[k]$가 정확히 일치할 가능성은 거의 없다. 그래서 둘 사이에 유사성이 있는지를 알아보기 위해 미리 주어진 T에 대해 $sim(w, w^*) > T$인지 아닌지를 결정한다. 물론 T값을 적절하게 설정하는 것은 고전적인 결정 (Decision) 또는 추정 (Estimation) 문제에 속한다. 이 값을 잘 설정함으로써 바로 이어 (2)절에서 설명될 타입 I 에러 (False Positive 또는 False Alarm) 및 타입 II 에러 (False Negative 또는 Missed Detection) 가능성을 모두 최소화하기 원한다. 상관관계와 유사도는 모두 $w[k]$와 $w^*[k]$의 내적 $(w \cdot w^*)$을 구하지만 후자는 $(w^* \cdot w^*)$으로 정규화시켰다는 점이 다르다. 이 정규화에 의해 유사도 사이의 공정한 비교가 가능하게 된다.

2. 상관관계 기반 워터마크 (원본 필요)

상관관계를 이용하는 워터마크 기법은 원본신호 $x[k]$에 직접 워터마크 $w[k]$를 더하거나 곱한다. 워터마크를 삽입

하는 것 이상으로 중요한 것은 삽입한 워터마크를 찾아내는 방법이다. Cox 등의 방법 [3]은 우선 워터마크신호 $w[k]$에 해당하는 $w^*[k]$를 추출한다. 그런데 $w^*[k]$를 추출하려면 원본신호 $x[k]$를 가지고 있어야 한다. 일단 수신신호 $r[k]$에서 $x[k]$를 제거하여 $r[k]-x[k] \approx w[k]+n[k]$를 만들고 이를 통해 $w^*[k] = w[k] + n[k]$를 만든다. 이어 $w[k]$와 $w^*[k]$의 유사도를 구해 T와 비교함으로써 워터마크가 삽입되어 있는지 아니면 워터마크가 부재인지를 판정한다. 즉 다음과 같은 비교절차를 거치게 된다.

$$\begin{cases} sim(w, w^*) > T & \text{워터마크삽입} \\ sim(w, w^*) > T & \text{워터마크부재} \end{cases}$$

그런데 이런 평가는 필연적으로 오류를 동반하게 된다. 그 오류는 그림 5에서 보는 바와 같이 앞서 기술한 것처럼 타입 I 에러와 타입 II 에러인데, 공격이나 신호처리과정에서 발생하는 각종 오류 때문에 피하기는 어렵다. 신호처리에서는 양자화, 압축, 잡음 등으로 인해 에러가 발생한다.

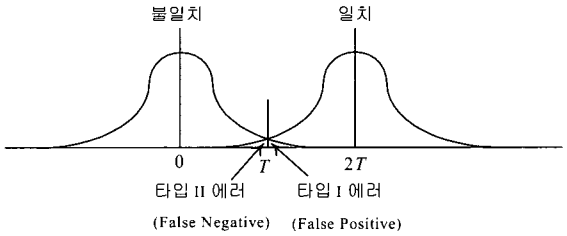

그림 5. 의사결정 과정에서 발생하는 확률적 에러 가능성
Fig. 5. Probabilistic errors due to imprecise decision making

원본 워터마크 $w[k]$와 추출된 $w^*[k]$가 우연히도 일치할 가능성도 있다. 그래서 유사도가 높다고 해서 두 신호가 비슷하다고 말할 수는 없다. 만일 $w[k]$가 정규분포 $N(0,1)$의 특성을 지니며 $w^*[k]$를 무작위로 선택했다고 가정하자. 이때 $w^* \cdot w$의 값은 $\sum_t^n w^*[k]w[k]$로 계산이 되는데 식의 유도를 편하게 하기 위해 Cox 등 [3]은 $w^*[k]$를 상수로 보았다. 결국 $w[k]$와 $w^*[k]$가 독립이며 $w[k]$가 정규분포 $N(0,1)$를 갖고 $w^*[k]$가 상수라는 조건에 의해 $w^* \cdot w$의 분포는

$$N\left(0, \sum_{t=1}^{n}[w^*[k]]^2\right) = N(0, w^* \cdot w^*) \qquad (9)$$

가 된다. 따라서 $sim(w, w^*)$는 $N(0,1)$분포를 갖게 된다. 이제 정규분포에서 표준 유의수준 검사를 시행할 수 있게 된다. 그러므로 T가 6이라는 것은 분산이 6이라는 것을 의미하므로 타입 I 에러가 발생할 확률은 거의 0에 가깝다.

3. 상관관계를 이용한 블라인드 워터마크 시스템

위의 방법을 쓰려면 워터마크 $w^*[k]$의 검출이 이루어져야 한다. 그런데 실제로 블라인드 워터마크에서는 $w^*[k]$의 검출이 불가능하다. 그래서 사본신호 $s[k]$에 고역필터 (High-Pass Filter), 저역필터 (Low-Pass Filter), 백색화 필터 (Whitening Filter)[7]등을 적용해서 $w^*[k]$를 추출하거나 $x^*[k]$를 추출하는 방법을 쓸 수 있다. 또는 오디오인 경우 LPC (Linear Predictive Coding) 기술을 적용해서 오디오 신호를 부분적으로 제거하기도 한다[9]. 이 경우 원본이 없어도 되므로 블라인드 워터마크를 만들 수 있다.

먼저 그림 6과 같이 고역필터를 써서 일단 신호성분 $s[k]$를 제거하고 $w^*[k]$를 추출하는 방법이 있다. 워터마크가 들어간 사본신호 $s[k]$의 모양은 그림 18과 같다. 원본신호 $x[k]$를 잘 제거할 수 있는 필터를 사용하면 신호성분 $x[k]$를 상당히 제거할 수 있다. 다른 한 가지 방법은 $s[k]$를 저역필터에 통과시켜 $x^*[k]$를 예측하고 $s[k]$와 $x^*[k]$를 빼서 둘의 차이를 추출한 워터마크라고 보는 방법이 있다.

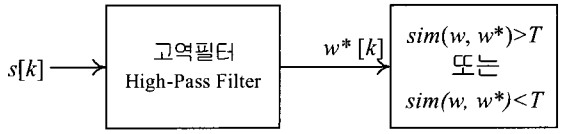

그림 6. 유사도를 이용하는 블라인드 워터마크 시스템 (고역필터를 쓴 경우)
Fig. 6. Blind watermarking system with high-pass filter based on the similarity

이런 방법의 한계는 사전에 어떤 형태의 필터로든 필터링을 해버리면, 예를 들어 $s[k]$가 저역필터를 통과한 출력이라서 이미 고주파 성분을 잃어버렸다면, $w^*[k]$는 워터마크 성분을 거의 포함하지 못한다. 따라서 이런 방법은 공격을 받지 않았을 때에 한해 쓸모가 있는 시간영역 삽입방법이라고 할 수 있다. 물론 삽입하는

워터마크를 어떤 필터링 공격에 잘 견디도록 만들면 강인성을 높일 수는 있다. 다만 그것이 쉽지 않다는 것이 문제이다.

4. 시간영역 숨기기

시간영역에서 워터마크를 숨기는 방법으로 Hartung과 Girod의 방법이 있다[6]. 이 방법은 신호 $x[k]$에 유사잡음 $w[k]$를 더해서 워터마크를 생성한다. 삽입하는 식은 다음과 같다.

$$s[k] = x[k] + sign(b) \cdot \alpha[k] \cdot w[k] \qquad (10)$$

여기서 b는 워터마크의 유무를 나타내는 심볼이며, $\alpha[k]$는 잡음 강도를 나타낸다. 잡음강도는 그 값이 작을수록, 즉 0에 가까울수록 원본의 품질을 적게 훼손하지만 워터마크를 추출할 수 있는 확률도 낮아진다.

워터마크 "1"을 숨기고 싶으면 $sign(b) = 1$로 하고, 워터마크 "0"을 숨기고 싶으면 $sign(b) = -1$로 잡는다. 워터마크를 검출할 때는 $s[k]$와 $w[k]$의 내적을 구해 그 값의 부호를 사용한다. 그 내적의 부호가 양수이면 $sign(b) = 1$로 워터마크 "1"이 있다고 판정한다. 그렇지만 내적의 부호가 음수이면 $sign(b) = -1$라고 보고 워터마크 "0"이 있다고 판정한다. 이런 근거는

$$\begin{aligned} s &= \sum_{k=1}^{N} s[k] \cdot w[k] = u + v, \\ u &= \sum_{k=1}^{N} x[k] \cdot w[k], \\ v &= sign(b) \cdot \alpha[k] \sum_{k=1}^{N} w[k] \cdot w[k] \end{aligned} \qquad (11)$$

의 식에서 u, 즉 $x[k]$와 $w[k]$의 내적이 0이 되며, v의 $w[k]$와 $w[k]$의 내적은 양수이고, 잡음강도 $\alpha[k]$는 원래 양수였으므로 결국은 s는 $sign(b)$에 의해 워터마크의 존재 유무를 판별하게 된다는 것이다. 그런데 이 방법이 지닌 가장 큰 문제는 $x[k]$와 $w[k]$의 내적이 0이 된다는 가정이 잘못되었다는 사실이다. 즉 이 내적은 신호의 특성에 따라 아주 큰 값을 생성시켜 둘째 항의 값 이상으로 커지게 될 수 있다. 즉 흔히 $u > v$인 상황이 발생해서 오류를 일으킬 수 있다. 일반적으로 워터마크의 길이가 매우 커지면 $u = 0$이 된다고 가정하지만 이것도 실제 실험을 통해 확인한 바에 의하면 그렇지 않았다. 그렇지만 $x[k]$에 따라 $u > v$가 되도록 하는 $w[k]$가 존재함을 확인할 수 있었다. 그런데 이처럼 영상에 따라 $w[k]$가 달라지면 워터마크를 검출할 때마다 어떤 워터마크를 삽입했는지 결정해야 하기 때문에 문제가 매우 복잡해진다.

5. 변환영역 숨기기

앞에서 살펴본 Hartung과 Girod의 방법[6]을 변환영역에서 적용할 수 있다. 이 방법은 오류를 발생시키지만 않는다면 원본을 필요로 하지 않는 블라인드 워터마킹 기법으로 쓸 수 있는 장점이 있다. 그런 면에서 블라인드 워터마킹 방법이 아닌 Cox 등[3]의 방법과 비교된다. 따라서 그림 6과 같은 시간영역에서의 필터링 기법을 쓰지 않아도 된다. 그런데 일단 $u = 0$이라는 조건만 성립한다면 Hartung과 Girod의 방법[6]도 변환영역에서 충분히 쓸 수 있다. 왜냐하면 $w[k]$는 $x[k]$와 무관하게 선정되었고, 따라서 $X[f]$와 $W[f]$도 무관하고, 당연히 식 (11)의 변환영역에서의 값 U는 0이 되면서 V의 부호로 워터마크를 판별할 수 있다. 식 (11)이 시간영역에서 성립한다면 식 (11)은 변환영역에서도 성립한다. 물론, 시간영역에서 나타나는 문제점이 변환영역에서도 그대로 나타난다.

Ⅳ. 패치워크 방법

패치워크 방법은 부분집합 X와 부분집합 Y를 선택해서 둘을 변조하는 방식을 택한다. 이 방법은 두 집합의 통계적 특성을 비교하는 방법이기 때문에 통계학에 대한 기본적인 배경이 필요하다. 앞서 살펴본 확산대역 기법 또는 상관관계를 이용하는 방법에 비해 적은 양의 워터마크 정보를 숨기면서 검출확률은 훨씬 높일 수 있는 방법이다. 초기 이론은 Bender, Gruhl, Morimoto와 Lu[2], Pitas와 Kaskalis[8]가 제안하고, Arnold[1]가 주파수 영역에 적용했으며, Yeo와 Kim[12] 등이 유용한 방식으로 개선하기에 이르렀다. 패치워크 방법도 실제로는 확산대역 기법이라고 볼 수 있다. 다만 검출하는 방법으로 상관관계 대신 통계적으로 평균 및 분산을 이용한다는 점이 다르다.

1. 패치워크의 개념

그림 7의 왼편 상단에 두 개의 상자가 보인다. 왼편 상자의 값은 주변의 픽셀보다 훨씬 어둡고, 그 옆의 상자는 약간 밝게 일부러 과장해서 표시했다. 부분집합 X를 하나의 패치라고 부르며, 부분집합 B도 하나의 패치라고 부른다. 패치 A는 원래의 픽셀 값에서 d를 빼고, 패치 B는 반대로 원래 픽셀 값에 d를 더한다. 워터마크를 삽입하는 것은 이와 같이 매우 단순하다. 그렇지만 워터마크의 평균과 분산을 구해야 하고, 워터마크가 숨겨진 위치를 정확히 알아야 하기 때문에 검출은 정교하고 복잡해진다. 즉 동기화(Synchronization) 문제가 발생한다. 모든 방법이 다 동기화 문제를 안고 있으나 특별히 패치워크가 동기화에 민감하다.

그림 7. 패치워크의 개념도. 두 부분집합 X와 Y의 선정 방법이 매우 중요하다.
Fig. 7. Conceptual figure for patchwork with two sets X and Y

그림 8. 패치워크를 위해 무작위로 두 부분집합의 위치를 선정하는 방법
Fig. 8. Random sampling for two sets for patchwork algorithm

실제로는 그림 7과 같이 집합을 인접한 점들로 구성하지 않는다. 인접한 점들로 부분집합 X를 구성하면 집합 X는 서로 비슷한 통계적 특성을 갖는다. 역시 인접한 점들로 구성된 부분집합 Y의 점들도 비슷한 특성을 지닌다. 그렇지만 부분집합 X와 Y사이의 통계적 특성은 무척 다르게 된다. 그런데 패치워크는 두 부분집합의 통계적 특성이 매우 비슷해야 비로소 제 기능을 발휘할 수 있다.

그래서 패치를 만들 때는 통계적으로 샘플을 무작위 추출하게 된다. 그림 8이 무작위로 샘플을 추출해서 만든 부분집합 X와 부분집합 Y의 원소 위치를 보여주고 있다. 이렇게 샘플을 선정하면 부분집합 안의 원소들은 그 값에서 큰 차이가 있을 수 있지만, 두 부분집합 사이의 통계적 특성은 비슷해진다. 따라서 무작위 샘플 추출이 매우 중요하다.

2. 패치의 요구조건

두 패치 집합이 통계적으로 다른 성질을 가지는가를 확인함으로써 워터마크의 삽입여부를 판정한다. 이러한 판정 과정에서 검출함수를 이용한 통계적 가설검정을 수행하게 된다. 가설검정을 하기 위해서는 검출함수에 대한 분포를 알아야 한다. 일반적으로 영상이나 오디오의 경우, 검출함수의 정확한 분포를 유도하는 것은 쉽지 않기 때문에 중심극한정리와 같은 정규근사 방법을 사용할 수 있도록 패치 원소를 적절히 추출한다. 통상적으로 중심극한정리를 적용하기 위해서는 30개 이상의 원소를 지닌 패치가 사용된다. 그러나, 샘플을 잘 선정하기만 하면 부분집합 원소의 개수가 필요 이상으로 클 필요가 없다. 샘플을 무작위로 뽑았을 때 샘플이 통계학적으로 가장 잘 선정되었다고 한다.

이 패치워크 기법의 모티브는 같은 모집단, 즉 한 영상이나 오디오에서 랜덤하게 선택된 확률 표본들의 두 부분집합은 통계적으로 비슷한 성질을 가진다는 것이다. 여기서 통계적 성질을 나타내는 모수로써 평균과 표준편차를 생각할 수 있다. 만약 강제적으로 각각의 집합에 워터마크를 삽입해 다른 특성을 갖도록 만든다면 이러한 작업을 하지 않은 집합들에서 특성을 비교했을 때와 확률적으로 다르게 나올 가능성이 커진다. 예를 들어, 모평균이 μ이고 표준편차가 σ인 모집단에서 각각 n개의 표본을 다음과 같이 $X=\{X_1, ..., X_n\}$과 $Y=\{Y_1, ..., Y_n\}$로 추출하였다고 하자. 통계적으로 볼 때, 이들 표본들이 랜덤하게 선택되었다면 이들 집합의 표본평균의 기대값은 각각 $E\{\overline{X}\}=\mu$, $E\{\overline{Y}\}=\mu$ 이기 때문에 두 표본평균의 차의 기대값은

$E\{\overline{X}-\overline{Y}\}=0$이 된다. 즉, 두 표본 평균간에는 통계적으로 차이가 없다. 그러나, 강제적으로 두 집합의 원소의 값에서 임의의 상수 d을 더하거나 뺀다면, 즉, $X'=X+d$와 $Y'=Y-d$로 만든다면 두 표본평균의 차의 기댓값은

$$E\{\overline{X}'-\overline{Y}'\}=E\{(\overline{X}+d)-(\overline{Y}-d)\}=E\{\overline{X}-\overline{Y}\}+2d=2d \quad (12)$$

과 같이 된다. 그림 9는 d=1일 때 $\overline{X}-\overline{Y}$의 분포를 보여준다. 여기서, $E\{\overline{X}-\overline{Y}\}=0$인 것을 근거로 $E\{\overline{X}'-\overline{Y}'\}=2d$임을 이용해서 d를 경계 (Threshold) T로 삼아 워터마크 유무를 판별한다.

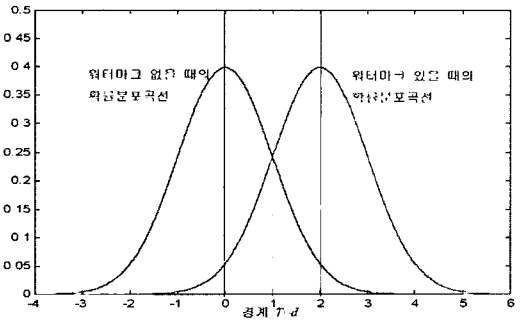

그림 9. 패치워크의 통계적 특성. $d=1$인 경우.
Fig. 9. Probability distributions with (right) and without (left) watermark.

3. 패치워크에서의 이슈

패치워크가 안고 있는 문제점은 $E\{\overline{X}-\overline{Y}\}=0$이지만 우리가 실제로 사용하는 중심 통계량 $\overline{X}-\overline{Y}$는 확률변수이기 때문에 표본이 어떻게 선택되는가에 따라 0보다 클 수도 있고 작을 수도 있다. 그러므로, 그림 9에서 보는 것과 같이 워터마크를 삽입하지 않은 분포의 경우에도 $\overline{X}-\overline{Y}$가 경계 T보다 크게 나올 수 있고 삽입했음에도 불구하고 $\overline{X}-\overline{Y}$가 경계 T보다 작게 나올 수 있다. 패치워크에서는 타입 I 및 II 에러 발생 가능성을 어떻게 줄이는가가 가장 중요한 이슈이다. 기본적으로, 삽입 전의 분포와 삽입 후의 분포의 거리가 멀어질수록 두 오류가 발생할 확률은 줄어들겠지만 d가 커지면 삽입한 부분이 많이 훼손될 가능성이 높아진다. 그러므로, 원본을 훼손시키지 않는 범위에서 두 오류의 확률을 줄이는 것이 패치워크에서 연구되어야 할 주요 문제이다. 그리고, 오류의 확률을 구하기 위한 통계량 $\overline{X}-\overline{Y}$의 보다 정확한 분포를 유도하는 방법과 오류가 발생할 확률을 줄이기 위해 같은 워터마크 정보를 반복하여 삽입하고 여러 번 검출한 후 결론을 내리는 방법들에 대한 연구 등이 필요하다.

4. 부호함수의 사용

패치워크에 상수 d를 더할 때 부호함수를 쓰면 위에서 지적한 타입 II 에러 발생문제를 해결할 수 있다. 실제로 구현하는 방법은 다음과 같다.

$$X'=X+sign(\overline{X}-\overline{Y})\cdot d,\ Y'=Y-sign(\overline{X}-\overline{Y})\cdot d \quad (13)$$

$\overline{X}-\overline{Y}$의 부호를 계산하고, 그 계산 결과에 따라 부호를 조정한다. 예를 들어 $\overline{X}-\overline{Y}$의 부호가 "+"이면 $\overline{X}$가 더 크다는 것을 의미하므로 이때는 $X'=X=d$처럼 X에 d를 더한다. $\overline{X}$가 더 커서 $X'=X+d$로 만들었으면 큰 것을 더 크게 만들고, $Y'=Y-d$처럼 작은 것을 더 작게 만드는 효과가 있다. 이것은 큰 것은 더 크게, 작은 것은 더 작게 만들어 둘 사이의 차이를 더 크게 만든다. $\overline{X}-\overline{Y}$의 부호가 "-"일 때는 $\overline{X}$가 더 작다는 것을 의미하므로 $X'=X=d$가 되게 한다. 그러므로 이번에는 $Y'=Y-d$가 된다. 여기서도 마찬가지로 큰 것은 더 크게, 작은 것은 더 작게 만들어 둘 사이의 차이를 더 크게 만든다. 그래서 부호함수를 쓰게 되면 두 집단의 평균 차이는 언제든지 $2d$만큼 벌어지게 만든다. 이 관계를 식으로 표현하면 다음과 같다.

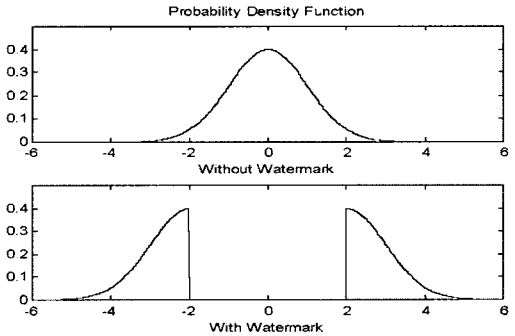

그림 10. 부호함수를 썼을 때의 확률밀도함수. 아래가 워터마크를 삽입한 경우로 $d=1$
Fig. 10. Probability distributions with sign functions

$$\overline{X}'-\overline{Y}'=\overline{X}-\overline{Y}+2d\cdot sign(\overline{X}-\overline{Y})\geq\overline{X}-\overline{Y}+2d \quad (14)$$

그래서 부호함수를 쓰면 대립가설 H_1의 확률분포 곡선이 그림 10의 아래처럼 주어진다. 이 그림은 $d=1$에 대한 특성을 보여주고 있다. 특이하게도 $[-2d, +2d]$에 해당하는 구간에서는 확률분포가 0이고 나머지 구간에서는 그림 38의 위에 있는 확률밀도함수를 반씩 잘라 좌우로 옮겨놓은 것과 같은 모양을 하고 있다. 이처럼 중간에 $-2d$에서 $+2d$사이가 0인 것은 부호함수가 언제나 두 부분집합의 평균을 $2d$만큼 벌려놓기 때문이다. 그러므로 워터마크가 삽입된 경우, 경계값 T를 $[-2d, +2d]$사이에서 선택하면 타입 II 에러가 발생할 확률은 0이 된다.

5. 패치워크의 통계적 성질

일반적으로 통계학에서 중요하게 여기는 두 값은 평균과 분산이다. 패치워크에서도 평균의 차이를 이용하는 방법과 분산을 이용하는 방법이 있다. 그리고 평균과 분산 모두 다 이용하는 방법이 있다. 일반적으로는 평균을 주로 이용한다[12]. 그것은 평균을 이용할 때 구현이 쉽기 때문이다. 이미 앞에서 설명한 것처럼 워터마크를 삽입하는 방법은 크게 가산형과 승산형이 있다. $X'=X+d$와 $Y'=Y-d$가 바로 가산형에 속한다.

가산형에서는 평균의 차이를 이용해서 워터마크의 유무를 검출한다. 그렇지만 승산형에서는 분산을 이용해 워터마크를 검출한다. 그런데 단순히 분산만을 이용하는 방법은 가산형에 비해 성능이 현저히 떨어짐을 실험을 통해 확인했다. 그래서 승산형은 개선의 여지가 아직도 많이 있다.

V. 에코 숨기기

에코 숨기기 아이디어는 Bender 등에 의해 처음 제안되었다[2]. 최근 오현오 등[13]이 에코 숨기기의 성능을 향상시킬 수 있는 듀얼 커널을 제안하기에 이르렀다. 에코 숨기기는 오디오에 적용할 수 있는 방법이다. 비디오에서는 에코를 숨기기가 쉽지도 않고, 숨겨도 눈에 이상이 쉽게 감지될 뿐 아니라, 검출도 어렵다. 에코는 시간영역에서 삽입한다. 에코는

$$s[k]=x[k]+\alpha x[k-d] \tag{15}$$

와 같이 삽입한다. 에코를 검출할 때는 주로 켑스트럼(Cepstrum) 함수를 이용한다[2][13].

에코 검출을 통해 얻을 수 있는 정보는 우선 에코의 유무이다. 만일 에코가 있다면, 비트 "0"이 삽입되었는지, 아니면 "1"이 삽입되었는지를 원점으로부터의 피크까지의 거리로부터 판단한다. 그림 11이 이런 상황을 설명해준다. 에코가 없으면 켑스트럼 피크가 (a)처럼 발견되지 않는다. 그렇지만 워터마크가 삽입되었을 때는 (b)나 (c)처럼 피크가 검출된다.

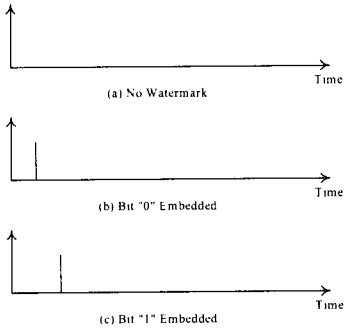

그림 11. 원점에서부터 피크까지의 거리를 이용한 에코 및 워터마크 비트 검출 개념
Fig. 11. Watermark detection with echo hiding using distance from the origin

그렇지만 에코를 삽입할 때 거리를 이용하면 에코를 넣을 수 있는 범위의 제한 때문에 다중 워터마킹에 많은 제약이 가해진다. 에코를 넣을 수 있는 범위보다 거리가 멀면 에코가 귀에 들리고, 짧으면 에코검출이 어려워진다. 특별히 워터마크를 검출할 때 오류로 인해 거리계산이 정확하게 이루어지지 못하면 다중 워터마킹이 더 어렵게 된다. 그래서 부호를 사용하는 방법도 있다. 그림 12가 부호를 이용한 삽입의 개념을 설명하고 있다. 이 방법은 워터마크 비트 "0"일 때는 아래로, "1"일 때는 위로 피크가 검출되도록 하는 방법을 말한다. 그러기 위해 워터마크를 심을 때는 식 (15) 대신 아래 식 (16)처럼 부호를 선정해야 한다. 마찬가지로 비트 "1"이면 "+" 부호를 택하고 "0"이면 반대 부호를 선택한다.

$$s[k]=x[k]\pm\alpha x[k-d] \tag{16}$$

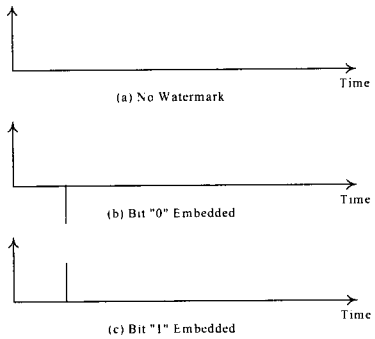

그림 12. 피크의 부호를 이용한 에코 및 워터마크 비트 검출 개념
Fig. 12. Watermark detection with echo hiding using sign of peak

일반적으로 켑스트럼 $c[k]$는

$$c[k] = F^{-1}((log_{complex}F(s[k]))^2) \quad (17)$$

형태의 함수를 사용한다. 여기서 F는 푸리에변환을, F^{-1}은 푸리에역변환을 의미한다. 오디오를 44.1kHz로 샘플링했을 때 100 샘플 정도 이후 에코 신호를 넣으면 귀에 잘 들리지 않고 오히려 음을 풍부하게 만드는 효과가 있다. 그런데 검출효과를 높이기 위해 식 (17) 대신

$$c[k] = F^{-1}(\log F(s[k]) \quad (18)$$

을 쓸 수 있다. 워터마크 삽입함수도 식 (16) 대신에

$$s[k] = x[k] + \alpha x[k-d] - \beta x[k-d-\triangle] \quad (19)$$

처럼 사용하는 방법이 있다[13]. 이때 $d \geq \triangle$인 다양한 $\triangle$를 선정해 성능을 개선시킬 수 있다.

VI. 워터마킹 방법의 비교

워터마킹 방법을 비교하는 것은 상당히 주관적일 수 있다. 같은 조건을 만들기가 어렵고 곡의 특성도 다르며, 샘플의 길이, 잡음의 강도, 공격방법에 따라 성능이 크게 달라질 수 있다. 그렇지만 여기서 제시하는 성능이 절대적 기준은 되지 못하지만 경험의 공유라는 차원에서 어느 정도 가이드라인이 될 수 있을 것으로 생각한다.

표 1은 오디오 워터마크에 적용할 때 세 기법 사이의 차이를 정리한 것이다. 이미지나 비디오에 대해서도 상관관계기반 기법과 패치워크 기법의 성능비교는 가능하지만 에코은닉과의 비교는 불가능하다. 오디오의 경우에도 구현방법에서 다양한 변수가 있어 일반적인 성능비교가 쉽지는 않다.

표 1. 오디오 워터마크에서의 성능비교
Table 1. Performance comparison of audio watermarking algorithms

	상관관계기반	패치워크	에코은닉
요구되는 잡음길이	긴 잡음	매우 적은 수의 샘플	
잡음저장공간	다량	소량	불필요
잡음삽입영역	주파수영역	주파수영역	시간영역
검출방법	자기상관관계	평균과 분산	켑스트럼
검출계산량	많다	적다	매우 많다
잡음삽입 위치동기	매우 민감	매우 민감	둔감
선형신호처리공격내성	강인	강인	강인
비선형신호 처리공격내성	매우 약함	매우 약함	약함
워터마크제거	곤란	매우 곤란	아주 용이
잡음 가청성	잡음영향 매우 큼	잡음 영향 미미	잡음 영향 미미

일반적으로 상관관계기반의 경우 오디오 샘플의 길이가 1,000 샘플이라면 1,000 샘플 길이의 잡음을 삽입한다. 잡음의 길이가 길수록 좋은 성능이 보장된다. 따라서 긴 잡음을 저장할 수 있는 공간이 필요하다. 잡음을 저장하지 않으려면 간단히 잡음을 재생할 수 있는 방법이 필요하다. 패치워크의 경우에는 두 집합 포함해서 50 샘플 정도에다만 잡음을 삽입한다. 따라서 패치워크의 경우에는 실제로 잡음을 저장하는 것이 아니라 잡음이 삽입될 위치정보를 저장해야 한다. 에코의 경우에는 잡음을 삽입하는 것이 아니고 에코를 이용하므로 잡음 자체를 저장할 필요는 없다. 상관관계기반 기법은 워터마크를 시간영역에서 삽입할 수도 있고 주파수영역에서 삽입할 수도 있다. 그러나 보통은 공격에 대한 내성을 높이기 위해 주파수영역에서 삽입한다. 패치워크의 경우에도 비슷한 이유로 주파수영역에서 삽입한다. 그렇지만 에코는 시간영역에서 삽입한다. 워터마크 검출에서는 패치워크가 가장 간단한 계산에 의존한다. 패치워크에서는 주파수영역으로 변환하는 계산량을 제외하면 워터마크가 삽입된 샘플의 평균과 분산을 구해 검출함수를 만들기 때문에 실제 계산량은 매우 적다. 상관관계기반 방법은 쉽게 잡음소리가 귀에 들리는 단점이 있다. 그래서 심리음향모델을 적용하지 않으면 실용성이 없다. 따라서 삽입단계에서는 심리음향모델도 계산해야 하므로 삽입단계에서의 계산량이 매우 많아지는 약점을 지니고 있다. 상관관계기반 기법에서는 주파수영역으로도 변환을 해야 하지만 자기상관계수도 구해야 하므로 검출 계산량이 많아진다. 그렇지만 검출단계에서는 심리음향모델 계산은 불필요하다. 에코의 경우에는 주파수영역으로 변환하지는 않지만 켑스트럼 자체의 계산량이 매우 많다.

워터마크를 삽입하기 시작한 위치를 정확히 아는 것이 워터마크 검출에 매우 중요하다. 상관관계기반 기법에서 사용하는 잡음은 거의 백색잡음에 가깝기 때문에 동기가 완전히 일치하지 않으면 워터마크를 전혀 검출하지 못한다. 패치워크도 위치가 어긋나면 워터마크 검출이 어렵다. 그렇지만 에코는 동기가 약간 어긋나도 워터마크의 유무를 판단할 수 있다. 따라서 에코는 동기를 맞추는 용도에 적용할 수도 있다. 특별히 에코는 선형속도변화 (Linear Speed Change) 또는 시간규모변경 (Time Scale Modification) 공격을 받았을 때 공격받은 정도를 유추하는 수단으로 매우 유용하게 쓸 수 있음을 실험을 통해 확인할 수 있었다. 세 기법 모두 선형공격, 예를 들면 필터

링, 잡음삽입, 압축 등에는 잘 견디는 것을 확인할 수 있었다. 그렇지만 비선형공격, 즉 선형속도변화 또는 시간규모변경 등의 공격에서는 오로지 에코만이 유일하게 저항할 수 있는 방법임을 실험을 통해 확인했다. 그렇지만 에코의 가장 큰 단점은 쉽게 삽입된 에코의 제거가 가능하다는 점이다. 일정한 크기의 샘플을 잡아 켑스트럼을 구해보면 쉽게 피크를 찾을 수 있고, 이로부터 에코가 있음을 확인하고 에코를 없애는 방법을 적용할 수 있다. 바로 이런 이유 때문에 에코를 이용해서 워터마크를 삽입하는 것은 매우 위험하다. 이에 비해 상관관계기반 방법이나 패치워크에서는 워터마크 제거가 상대적으로 어렵다.

Ⅶ. 맺음말

이 논문에서는 블라인드 워터마크로 사용되는 상관관계기반 방법, 에코기반 방법, 패치워크 방법에 대해 개괄적으로 살펴보았다. 워터마크에 대해 많은 논문이 발표되었지만[1][2][3][4][5][6][7][8][9][10][11][12][13][14][15], 현실적으로 블라인드 워터마크를 삽입하고 검출하는 방법은 의외로 그 수가 적고 종류도 많지 않다. 특별히 본 논문에서는 블라인드 워터마크로서 상관관계기반 방법은 Hartung과 Girod의 방법[6], 패치워크의 경우 Yeo와 Kim의 방법[12], 에코는 오현오, 김현욱, 윤대희, 석종원, 홍진우의 방법[13]을 기준 방식으로 참조했다.

상관관계 기반 방식은 Hartung과 Girod의 방법[6]에 의해 비로소 블라인드 워터마킹 기법의 틀을 갖추었다. 이에 비해 패치워크나 에코는 그 자체로 블라인드 워터마킹 기법이 될 수 밖에 없었다. 각각의 방법에 대해 공정하게 성능을 비교하는 것이 어렵지만 참고자료 수준으로 성능비교 자료를 제시했다.

본 논문에서는 지면의 제한으로 실험한 방법에 대해 자세히 기술하지 못했고 참고문헌도 충분히 나열하지 못했다. 그렇지만 대부분의 독자는 이상의 설명만으로도 쉽게 실험을 재현할 수 있을 것으로 예상한다. 더 많은 자료를 원한다면 IEEE 특집호 [14][15]를 참조하면 된다. 이 논문에 결과만 요약해서 기술한 실험 내용은 별도의 논문으로 작성해서 발표할 예정이다.

참 고 문 헌

[1] M. Arnold, "MP3 robust audio watermarking," *Proceeding of the 2000 IEEE International Conference on Multimedia and Expo*, vol.2, pp.1013-1016, 2000.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol.35, no.3&4, pp.313-336, 1996.

[3] I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol.6, pp.1673-1687, 1997.

[4] S. Craver, N. Memon, B.-L. Yeo, and M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications," *IEEE Journal of Selected Areas in Communications*, vol.16, no.4, pp.573-586, 1998.

[5] J. J. Eggers, J. K. Su, and B. Girod, "A blind watermarking scheme based on structured *codebooks," Proceedings of the IEE Secure Images and Image Authentication*, 2000.

[6] F. Hartung, F. and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing*, vol.66, no.3, pp.283-301, 1998.

[7] H. Kim, Stochastic Model Based Audio Watermark and Whitening Filter for Improved Detection, M.S. Thesis, School of Electrical Engineering, *Seoul National University*, 2000.

[8] I. Pitas and T. H. Kaskalis, "Applying signatures on digital images," *Proceedings of the IEEE Workshops on Nonlinear Image and Signal Processing*, pp. 460-463, 1995.

[9] J. W. Seok and J. W. Hong, "Audio watermarking for copyright protection of digital audio data," *Electronics Letters*, vol.37, no.1, pp.60-61, 2001.

[10] A. Tirkel, G. Rankin, R. van Schyndel, W. Ho, W., Mee, N., and Osborne, C., "Electronic water mark," *Proceedings of the DICTA 1993*, pp.666-672, 1993.

[12] I. K. Yeo and H. J. Kim, "Modified Patchwork Algorithm: The Novel Audio Watermarking Scheme," *Proceedings of the IEEE International Conference on Information Technology: Coding and Computing, Las Vegas, Nevada*, pp.237-242, 2001.

[13] 오현오, 김현욱, 윤대희, 석종원, 홍진우, "강인한 오디

감사의 글

KAIST의 IDEC이 ISMC 연구회를 통해 지원해주신 점에 대해 감사드립니다. 논문을 의뢰해주신 특집 편집위원 홍진우 박사 (ETRI), 그리고 논문의 질을 높이는데 도움이 된 심사위원들의 권고에 감사드립니다. 그리고 실험을 통해 여러 사실들을 검증해준 강원대 대학원생들에게도 감사드립니다.

오 워터마킹을 위한 새로운 반향 커널 설계", *한국음향학회지*, 20권, 2호, pp.66-76, 2001.
[14] *IEEE Signal Processing Magazine*, vol.17, no.5, 2000.
[15] *Proceedings of the IEEE*, vol.87, no.7, pp.1057-1308, 1999.

저 자 소 개

김 형 중

1978년 : 서울대 전기공학과(공학사)
1986년 : 서울대 제어계측공학과(공학석사)
1989년 : 서울대 제어계측공학과(공학박사)
1992년~1993년 : USC 방문교수
1998년~2000년 : 중기거점 과제(iPCTV)개발 총괄책임자
2000년~현재 : 중기거점과제(iMS)개발 총괄책임자, 강원대학교 교수

여 인 권

1992년 : 성균관대학교 통계학과(학사)
1997년 : University of Wisconsin-Madison 통계학과 (Ph.D.)
1999년~2000년 : 강원대학교 인턴연구원(과학재단 지원)
현재 : 강원대학교 객원교수(정보통신연구관리단 지원)