워터마크를 이용한 멀티미디어 컨텐츠의 저작권 보호

Copyright Protection of Multimedia Contents Using Watermark

석종원(J.W. Seok) 실감AV연구팀 선임연구원
홍진우(J.W. Hong) 실감AV연구팀 책임연구원

디지털 워터마크는 디지털 데이터에 삽입된 후 검출되거나 추출될 수 있도록 원신호에 추가된 신호를 의미한다. 디지털 서명(signature)이라고 말하기도 하는 워터마크는 디지털 데이터에 삽입된 일종의 패턴으로써, 디지털 멀티미디어 저작물의 저작권 보호를 위해 최근 들어 활발히 연구되고 있는 분야이다. 본 고에서는 멀티미디어 데이터의 소유권을 보호할 수 있는 워터마킹 기술의 역사와 정의 및 응용범위, 워터마크가 갖추어야 할 조건들, 그리고 문자, 영상 및 오디오 데이터의 워터마킹 기술에 대해 살펴보았다.

I. 서 론

인터넷과 같은 컴퓨터 망과 컴퓨터 이용의 급격한 발달로 인하여 문서, 음성, 오디오, 영상, 동영상 등의 멀티미디어 데이터의 이용 및 보급이 일반화되고 있다. 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. 이에 불법적인 복제를 방지하고 멀티미디어 컨텐츠를 생산해내는 작가의 저작권 및 소유권을 보호하고자 하는 요구가 생겨나게 되었다.

지금까지 가장 대표적이고 널리 사용되는 데이터 보호기법은 데이터를 암호화(encryption)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(watermarking) 기법이 디지털 멀티미디어 컨텐츠 저작권 보호를 위한 새로운 해결책으로 제시되고 있으며, 국내외에서 이와 관련된 연구가 활발히 진행되고 있다.

본 고에서는 멀티미디어 컨텐츠 보호를 위해 사용되는 대표적인 워터마킹 기법들을 소개하였다. 멀티미디어 컨텐츠의 속성상 각각의 컨텐츠는 각기 다른 방법으로 워터마크가 내장되어야 하므로 워터마킹 기법들을 문서, 오디오, 그리고 영상에 따라 분류하고 이들을 서로 비교하였다.

II. 워터마크의 역사와 정의 및 응용 분야

1. 워터마크의 역사

워터마킹 기법은 Steganography 기법의 구체화된 한 형태이며 "감추어져 있다"는 뜻의 그리스어 말인 "stegano"와 "통신하다" 라는 뜻의 "graphos"가 결합된 단어이다. 최초의 워터마크 기록은 종이

에 새겨진 워터마킹 기법으로 약 700년 전으로 거슬러 올라가게 된다. 13세기 말 무렵에 이탈리아의 Fabriano에서는 약 40여 개의 제지공장들이 난립하고 있었다. 이들 공장에서 생산되는 종이는 형태나 질, 그리고 가격에 있어서도 천차만별이었다. 그리고, 이들 공장에서 생산되는 종이들은 완제품이 아니라 중간단계의 제품이었고, 중간단계의 종이는 공예가들이 후처리를 하여 최종적인 종이를 판매하게 되었다. 따라서, 공예가들은 각자의 제품에 대한 출처, 형태 및 종이의 질에 대한 정보를 가지는 고유한 워터마크를 종이에 삽입하게 되었고, 이러한 워터마킹 기술은 유럽 전체로 급속히 전파되었다[1].

본격적인 디지털 워터마크의 개념은 1990년대 초에 정립되었고, 최근에 널리 사용되고 있는 워터마크라는 용어는 1993년도에 Tirkel이 “water mark”라는 용어를 사용한 것이 계기가 되었다[2]. 이때부터 워터마킹 기법은 많은 관심을 끌게 되었고, 관련 기술도 급속도로 발전하게 되었다. <표 1>은 INSPEC에서 1992년부터 1998년까지 발표된 워터마킹과 관련되어 발표된 논문의 편수를 나타내고 있다[3]. 표에서 발표된 논문 편수가 매우 급격하게 증가하고 있음을 확인할 수 있다.

<표 1> 디지털 워터마킹 기법과 관련된 논문 편수

연도	1992	1993	1994	1995	1996	1997	1998
발표 편수	2	2	4	13	29	64	103

2. 워터마크의 정의

디지털 워터마크는 디지털 데이터에 삽입된 후 검출되거나 추출될 수 있도록 원신호에 추가된 신호를 의미한다. 디지털 서명(signature)이라고 말하기도 하는 워터마크는 원신호의 매체에 가시성(visible) 또는 비가시성(invisible)의 신호를 추가함으로써 디지털 데이터에 삽입된 일종의 패턴으로써, 디지털 멀티미디어 저작물의 저작권 보호를 위해 제안되었다. 워터마크는 크게 2가지 형태의 기법이 있는데 가시성 워터마크와 비가시성 워터마크이다. 가시성 워터마크는 저작물의 소유를 가시적으로 명확히 나타나도록 표현하는 기법이며, 비가시성 워터마크는 원신호와 거의 구분할 수 없도록 저작물의 소유권을 은폐시키는 기법이다. 오늘날의 디지털 워터마킹 기법에 대한 연구는 대부분 비가시성 워터마크 기법에 집중되고 있으며 MPEG(Moving Picture Experts Group), SDMI(Secure Digital Music Initiative) 등에서 표준화 기법을 규정하기 위한 연구가 진행되고 있다.

3. 워터마크의 응용

가. 가시성 워터마크를 이용한 컨텐츠의 지적소유권 보호

영상 데이터에 소유권자의 가시성 워터마크를 삽입하고 그 영상을 다른 목적에 사용하는 것을 금지하지 않는다. 여기서 가시성 워터마킹이란 영상 내에 소유권자의 마크를 눈에 띄기 쉽게 삽입하는 것이다. 예를 들어 영상에 자신의 이름을 크게 새기거나 회사의 로고를 눈에 띄게 삽입하는 것을 생각할 수 있다. 가시성 워터마크의 목적은 영상의 상업적인 사용이나 지적소유권을 쉽게 알리기 위함이다.

나. 인증을 위한 컨텐츠의 지적소유권 제어

방송사 기자가 뉴스 방송을 위해 디지털 카메라로 찍은 비디오가 있다고 생각해 보자. 이 비디오를 사용하기 전에 방송국은 이 비디오가 수정되었거나 변조되지 않았는지 검증하기를 원한다. 이러한 검증을 위하여 비가시성 워터마크가 카메라로 비디오를 찍을 당시에 자동적으로 삽입된다. 여기에 삽입된 워터마크는 이 비디오가 변조되지 않았음을 증명한다.

다. 무단 배포 방지

저작물을 구매한 소비자가 무료로 타인에게 저작물을 복사하여 제공할 수 있다. 이는 저작권자의 저작권료의 감소를 초래한다. 저작권자는 이를 방지하기 위하여 저작물에 워터마크를 삽입한다. 저작권자 또는 그의 대리인은 저작물의 무료 배포를 방지하기 위하여 인터넷을 통해 공개된 저작물들에 대해 저작

권자의 워터마크가 삽입되어 있는지를 확인하여 불법 사용 여부를 판단한다.

라. 불법 배포자의 확인

저작권자는 무단 배포의 방지뿐만 아니라 무단 배포자가 누구인지 알기를 원할 것이다. 이를 위해서 저작물을 판매할 때 누구에게 판매하는지에 대한 정보를 비가시성 워터마크로 삽입한다. 불법 배포된 저작물이 적발되면 적발된 저작물에서 워터마크 검출을 통해 구매자의 정보를 알 수 있다. 이러한 정보는 저작권자는 구매자의 불법배포 사실을 증명할 수 있으므로 적절한 보상을 받을 수 있다. 이러한 응용의 가장 큰 특징은 저작물에 삽입되는 워터마크가 구매자에 따라 모두 다르다는 점이다. 이를 위해서는 굉장히 많은 수의 서로 다른 워터마크를 발생시킬 수 있어야 한다.

III. 워터마킹 기법이 갖추어야 할 요건

1. 비지각성(Imperceptibility)

몇몇 응용에서는 가시성 워터마크가 사용되지만 대부분의 응용에서는 비가시성 워터마크가 사용된다. 그래서 현재 워터마킹 기술에 대한 연구는 대부분 워터마크를 보이지 않게 또는 들리지 않게 영상이나 오디오 신호 속에 숨기는 방식들에 대한 것이다. 이것은 지적 소유권의 주장을 위해 워터마크를 삽입하면서도 서비스의 품질을 떨어뜨리지 않게 하기 위함이다. 예를 들어, 워터마크가 음악에 삽입되었을 때 원래의 음악과 워터마킹된 음악 사이의 차이를 청취자가 구별할 수 없을 정도여야 하며, 영상 또는 비디오의 경우에도 마찬가지로 화질의 차이를 느낄 수 없어야 한다. 만약 음질이나 화질의 차이가 발생한다면 소비자로부터 그 제품은 외면당할 수 있기 때문이다.

2. 강인성(Robustness)

디지털 형태의 음악, 영상, 비디오 등은 손실 부호화, 필터링, 크기변환(resizing), 대비강화(contrast enhancement), 클로핑(cropping), 회전(rotation) 등의 신호처리에 의해 쉽게 변형될 수 있다. 워터마킹 기술이 그 기능을 발휘하기 위해서는 그 워터마크가 위와 같은 신호처리 후에도 검출이 가능해야 한다. 신호처리에 강인한 워터마킹을 위해서는 워터마크가 신호의 중요한 부분에 삽입되어야 한다는 것이 일반적인 경향이다. 워터마크가 삽입된 데이터에 대한 공격(attack)은 원신호에 큰 변형을 주지 않고 워터마크만을 제거하려는 데 그 목적이 있다. 그래서 대개의 경우 저대역필터(lowpass filter)를 사용하거나 압축과정을 수행 후 고주파 성분을 제거하는 방법으로 공격이 이루어질 것으로 예상된다. 따라서 신호의 중요부분에 워터마크를 삽입함으로써 공격으로부터 제거되지 않도록 함이 타당하다. 한편, 변위(translation), 크기변환, 회전, 클로핑 등의 기하학적 변환(geometric transformation)이 영상에 가해지는 경우, 워터마크의 강인성은 상당히 약한 편이기 때문에 많은 보완이 필요하다. 워터마킹 기술이 영상, 오디오, 비디오와 같은 멀티미디어 저작물에 대한 지적 소유권 보호를 위해 성공적으로 적용되기 위해서는 강인성이 무엇보다 중요하다.

3. 삽입될 수 있는 정보의 양

워터마킹 알고리즘들은 대개 수동적으로 정한 일정량의 정보를 삽입하게 된다. 그러나 자동적으로 비지각성과 강인성 등의 특성을 만족하면서 삽입될 수 있는 정보의 양을 결정하는 알고리즘이 필요하다. 워터마크가 삽입된 영상이나 음악을 판매할 경우, 각 저작물에 저작물의 번호, 구매자에 대한 정보 등을 수록하기 위해서는 사용 가능한 워터마크의 수가 충분해야 하고, 이를 서로 구별하기 위해서는 삽입되는 정보의 양이 충분히 클 수 있어야 한다.

4. 워터마크의 검출 시 원신호의 사용 여부

워터마킹 기법은 원신호를 사용하는지 여부에 따라 크게 두 부류로 나누어볼 수 있다. 우선 원신호를 사용하여 워터마크을 검출하는 부류이다. Swan-

son[4]과 Wolfgang[5] 등의 연구가 이러한 접근방식을 사용한 경우이다. 이 연구들에서는 워터마킹을 제거하거나 검출할 수 없도록 데이터를 조작하는 기법들을 제안하고 있다. 그러나 이 방법은 실용적으로 적용하기 부적합하다. 왜냐하면 원신호가 유효하지 않은 경우가 존재할 수 있고, 신호처리 없이도 가짜 워터마크를 단순히 삽입함으로써 올바른 소유권자를 구별할 수 없도록 만들 수 있음이 지적되었기 때문이다[6, 7].

또 다른 부류는 원신호를 사용하지 않고 워터마크를 검출하는 부류이다. 이 방식을 Blind 방식이라고 부른다[8]. 최근 보고된 Blind 워터마킹 기법들이 많이 있지만[8-11] 보통의 영상처리에 의해 워터마크가 쉽게 제거 또는 파괴되는 단점을 가지고 있다. 그래서 좀 더 강인한 워터마킹 기법의 개발이 과제이다.

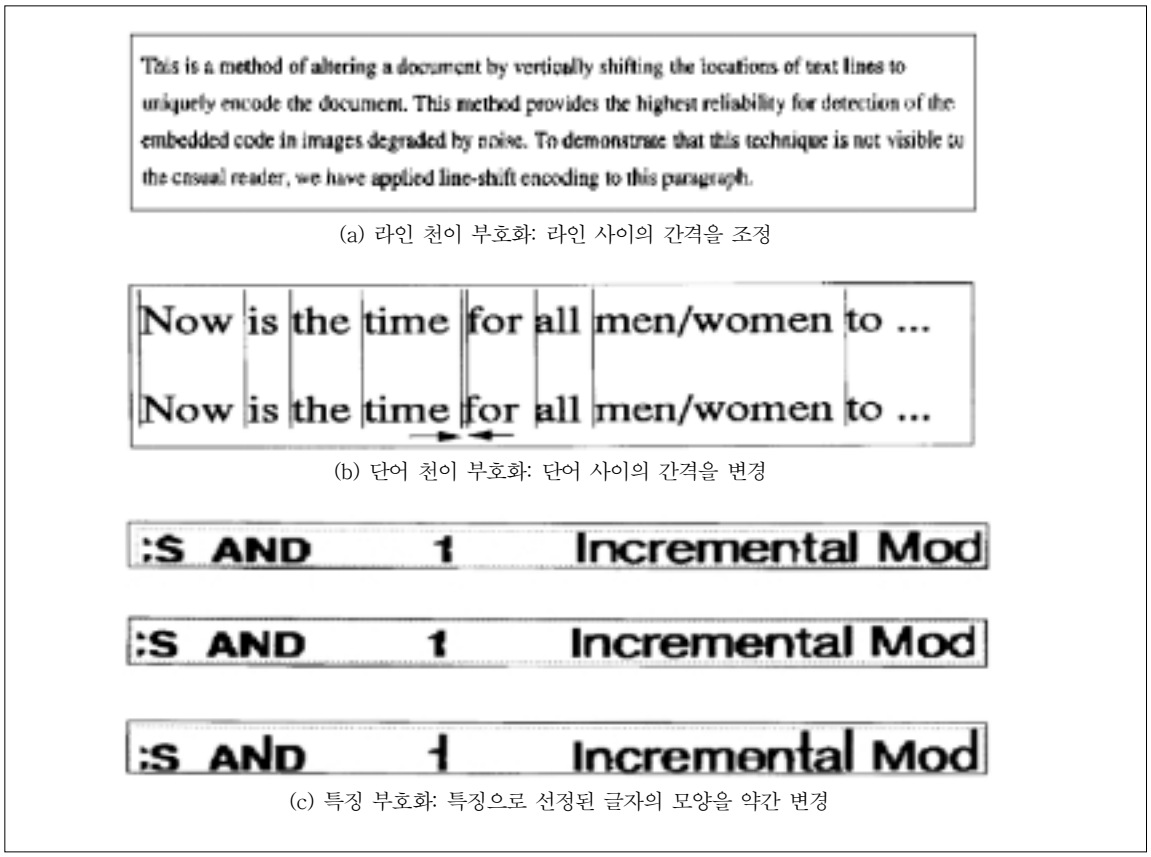
Ⅳ. 문서 데이터의 워터마킹

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. 가상 디지털 도서관 사용자는 2진 영상으로 저장된 전자문서나 책 등에 대해 사용권한을 부여 받은 후 다운로드할 수 있다. 하지만 다운로드한 문서는 삽입된 워터마크로 인해 다른 사람에게 배포할 수 없게 되거나 일정기간이 지나면 자동으로 문서가 소멸되게끔 하여 불법복제로부터 보호받을 수 있게 된다.

문서 데이터 워터마킹 기법은 Brassil에 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[12]. 라인 천이 부호화는 문서에 있는 라인들의 간격을 위와 아래로 조금씩 이동시키는 방법이다. 이때 문서에 저장되는 워터마크 정보는 각각의 라인이 움직인 방법에 의해 결정되게 된다. 단어 천이 부호화의 경우에는 라인 사이의 간격을 움직인 것과 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 내장시킨다. (그림 1)은 위에서 설명한 세 가지 문서 데이터 워터마킹 기법에 대한 예를 보여주고 있다. (그림 1a)는 라인 천이 부호화의 예로써 언뜻 보기에는 거의 차이가 나지 않을 정도의 간격 차이를 라인과 라인 사이에 두어 정보를 삽입하게 된다. (그림 1b)의 경우는 단어와 단어 사이의 여백에 차이를 두어 정보를 내장한 단어 천이 부호화의 예이다. (그림 1c)는 특징 부호화를 약간 과장된 형태로 표현한 경우로써 특징으로 선정된 특정 문자의 모양을 정해진 규칙대로 변경하여 정보를 내장한 예를 보여주고 있다. (그림 1c)에서 숫자 '1,' 문자 't' 그리고 'd'를 보면 그 형태가 조금씩 변형된 것을 확인할 수 있다.

Ⅴ. 영상 데이터의 워터마킹

지금까지 워터마킹과 관련된 연구의 대부분은 영상 데이터에 집중되어져 왔다. 현재까지 발표된 영상 데이터의 워터마킹 기법은 크게 두 가지 부류로 나누어 볼 수 있다. 하나는 워터마크를 공간영역(spatial domain)인 영상 데이터에 직접 내장하는 방법이고, 다른 하나는 영상 데이터를 DCT(Discrete Cosine Transform)나 DWT(Discrete Wavelet Transform)를 이용하여 변환한 다음 주파수 영역(frequency domain)에서 워터마크를 내장하는 방법이다. 본 장에서는 지금까지 발표된 많은 영상 데이터 워터마킹 기법 중 가장 널리 알려지고 여러 논문에서 많이 인용되는 공간영역에서의 워터마킹 기법인 Tirkel[2]이 제안한 알고리즘과 주파수 영역에서의 워터마킹 기법인 Cox[13]의 알고리즘에 대해 각각 설명한다.



(a) 라인 천이 부호화: 라인 사이의 간격을 조정

(b) 단어 천이 부호화: 단어 사이의 간격을 변경

(c) 특징 부호화: 특징으로 선정된 글자의 모양을 약간 변경

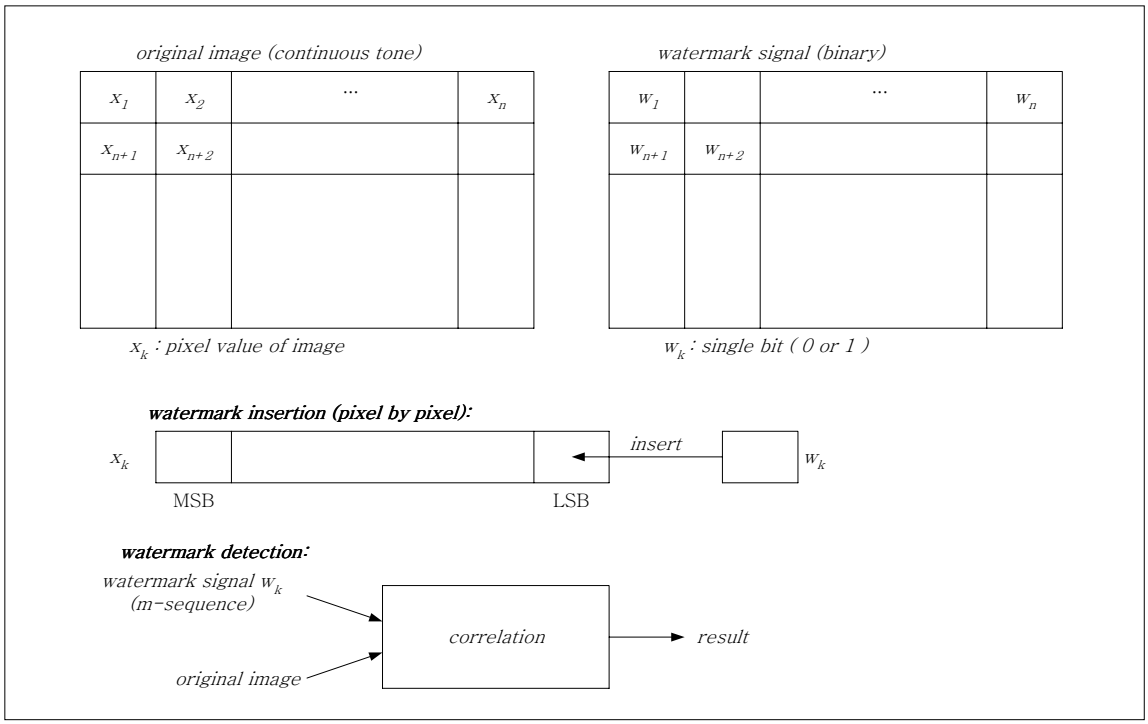
(그림 1) 문서 데이터의 워터마킹 예

1. 공간영역에서의 워터마킹

앞에서도 언급하였듯이 Tirkel은 "Watermark"라는 용어를 처음으로 도입하였고 그가 발표한 워터마킹 기법은 이후에 연구되어진 여러 형태의 워커마킹 연구에 있어서 기본이 되었다고 볼 수 있다. 이 알고리즘은 공간영역에서 영상 데이터를 표현하는 각각의 픽셀(pixel)값을 이진수로 표현한 다음 이중 LSB(Least Significant Bit)에 워터마크를 직접 내장하는 방법이다. LSB에 워터마크를 내장하는 이유는 워터마크를 내장한 후에 발생할 수 있는 영상의 열화를 최소화하기 위해서 이다. 이 알고리즘에서 이진수로 표현된 픽셀에 내장되는 워터마크는 당연히 이진수로 표현되어야 한다. 워터마크 검출 시에는 미리 저장된 워터마크와 워터마크가 내장된 영상에서 추출한 추정된 워터마크간에 상관관계를 이용하여 실제 워터마크가 내장되었는지를 판단하게 된다. (그림 2)는 Tirkel이 제안한 공간영역에서의 워터마킹 과정을 나타내고 있다. 이 외에도 Bender는 영상에서 픽셀값 두 개를 선택한 후 일정한 양만큼 하나의 픽셀은 감소시키고 다른 하나의 픽셀은 증가시키는 Patch Work 방법을 제안하였다[14]. Pitas는 영상을 크기가 같은 두 집합으로 나누고 한 집합의 픽셀 값들을 일정한 크기로 더하는 방법을 제안하였다[9]. 내장된 워터마크를 검출하기 위해서는 두 집합에 속한 픽셀들의 평균값의 차를 검정 통계량으로 하는 가설 검정 이론을 사용하여 워터마크를 검출하게 된다.

2. 주파수 영역에서의 워터마킹

현재 대다수의 워터마킹 알고리즘은 DCT나 DWT



(그림 2) 공간영역에서 영상 데이터의 워터마킹

와 같은 주파수 영역에서 워터마크를 삽입하고 있다. 과거의 워터마킹 기술이 알고리즘의 비공개에 주로 의존해 온 반면 Cox의 방식은 알고리즘을 공개할 수 있다는 점에서 기술적으로 큰 변화를 가져온 계기가 되었다[13]. 이 방식에 있어서 워터마크란 백색잡음을 의미하고 이 백색잡음은 슈도랜덤 수(pseudo-random number)이다. 이 슈도랜덤 수를 발생시키는 시드(seed)가 워터마크를 찾아내는 키(key) 역할을 한다. Cox의 방법은 워터마크 검출 시 원영상과의 차를 이용한다는 점에서 약점이 존재하지만, 이 방식은 현재 연구되고 있는 대부분의 워터마킹 기술에서 수정되어 사용되고 있으며 다음과 같은 알고리즘으로 구성되어 있다.

가. 워터마크의 발생

워터마크 w(n)는 식(1)과 같이 자기상관함수가 임펄스 형태로 나타나는 백색잡음이다.

$$R_w(\tau) \equiv E[w(n+\tau)w(n)] = \sigma_w^2 \delta(\tau) \qquad (1)$$

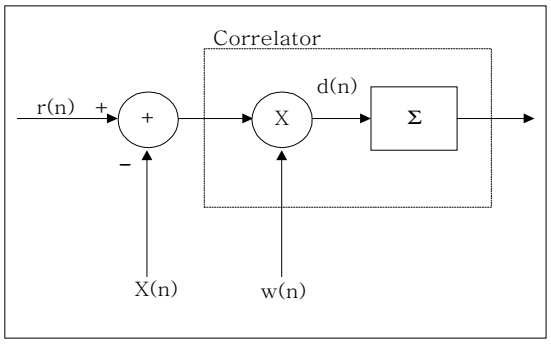
이 잡음의 분포는 워터마크를 설계하는 사람이 정할 수 있다. 대개의 경우 균일 분포(uniform distribution)나 가우시안 분포(Gaussian distribution)가 사용된다.

나. 워터마크의 삽입

워터마크의 삽입에 있어서 고려하여야 할 가장 중요한 사항은 비지각성과 강인성이다. 우선 비지각성의 특성을 만족하기 위하여 워터마크의 크기는 영상의 신호에 비해 상대적으로 굉장히 작도록 설정하여야 한다. 즉, σ_w^2 가 작도록 정해줘야 한다. 또한 원영상의 주파수 성분 중, 크기가 큰 주파수 성분에 워터마크의 크기를 크게 삽입하고, 크기가 작은 주파수 성분에는 워터마크의 크기를 작게 삽입한다. 즉,

$$w'(n) = \alpha |X(n)| w(n) \qquad (2)$$

여기서, α는 상수이고 X(n)은 워터마크를 삽입하



(그림 3) 워터마크의 검출

고자 하는 영상 신호의 n번째 주파수 성분이다. 식(1)과 식(2)에서 편의상 워터마크와 영상신호를 1차원적으로 표현하였다. 식(2)에서 얻어진 워터마크 $w'(n)$이 실제로 신호에 삽입된다. 여기서, $w'(n)$의 σ_w^2는 α와 $|X(n)|$에 의해 결정된다.

그리고, 워터마크가 삽입되는 주파수 영역은 공격에 강하고 공격이 가해졌을 때 영상 신호의 화질을 크게 손상시킬 수 있는 영역이어야 한다. 주파수 영역은 크게 저주파 대역과 고주파 대역으로 나누어 볼 수 있다. 고주파 대역에 워터마크가 삽입될 경우 공격으로부터 쉽게 워터마크가 제거될 수 있다. 가장 손쉬운 방법으로는 저대역통과필터를 사용하는 것이다. 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 저주파 대역에 집중되어 있어 영상 화질에 큰 저하를 가져온다. 그래서 Cox는 영상을 2차원 DCT를 수행한 후 저주파 대역이면서 주파수 성분의 크기가 큰 N개의 성분에 대해 워터마크를 삽입하였다.

$$X'(n) = X(n) + \alpha |X(n)| w(n) \qquad (3)$$

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

다. 워터마크의 검출

워터마크의 검출은 워터마크가 삽입된 신호와 워터마크 사이의 상관성을 구함으로써 쉽게 이루어질 수 있다. (그림 3)은 워터마크의 검출을 도식적으로 나타낸 것이다. 예를 들어, 시험하고자 하는 입력 신호를 $r(n)$이라고 하고 워터마킹된 영상 신호를 $X(n)+w(n)$이라고 하자. 이 때, 워터마킹된 신호가 일반적인 신호처리에 의해 왜곡이 일어난 경우, 입력 신호는 다음과 같이 쓸 수 있다.

$$r(n) = X(n) + w(n) + N(n) \qquad (4)$$

여기서, $N(n)$은 왜곡 성분이다. 우선 입력 신호와 원영상 신호와의 차이를 구하고 이 차신호에 대해 워터마크와의 상관성을 구함으로써 상관계수가 크면 워터마크가 검출된 것으로 결정하고, 작을 경우 검출되지 않은 것으로 결정한다. 검출기의 출력은 다음과 같다.

$$\begin{aligned} O(n) &= \frac{1}{L}\sum_{n=0}^{L-1}[(X(n)+w(n)+N(n)) - X(n)]\cdot w(n) \\ &= \frac{1}{L}\sum_{n=0}^{L-1} w^2(n) + \frac{1}{L}\sum_{n=0}^{L-1} N(n)w(n) \end{aligned} \qquad (5)$$

여기서, L은 워터마크의 길이이다. 식(5)의 두 번째 항에서 $N(n)$와 $w(n)$은 서로 상관성이 없으므로 상당히 작은 값을 가진다. 확률적으로 $E[\sum N(n)w(n)] = 0$이다. 그래서, 워터마크의 길이가 충분히 길 경우, 즉, $L \to \infty$일 때, $\frac{1}{L}\sum N(n)w(n) \to 0$이다. 따라서, 검출기는 워터마크가 존재하는지, 하지 않는지를 검출한다(그림 3).

(그림 4a)는 원본 lena 영상이며, (그림 4b)는 Cox의 알고리즘을 이용하여 워터마크를 내장한 영상이다. 두 영상의 시각적인 차이를 거의 느낄 수 없다. (그림 4c)와 (그림 4d)는 Cox 알고리즘에 공격을 가했을 경우에 대한 예를 보여주고 있다. (그림 4c)는 워터마크가 내장된 영상을 150×150으로 간축(decimation)한 후 다시 원래의 크기인 256×256으로 선형보간(linear interpolation)한 후의 유사도(similarity)와 상관계수(correlation coefficient)를 나타내고 있다. (그림 4d)는 가우시안 잡음을 첨가한

(a) 원본 lena 영상

(b) 워터마크가 내장된 영상
similarity: 30.12
correlation coefficient: 0.9621

(c) Resized(150×150) 영상
similarity: 23.76
correlation coefficient: 0.7032

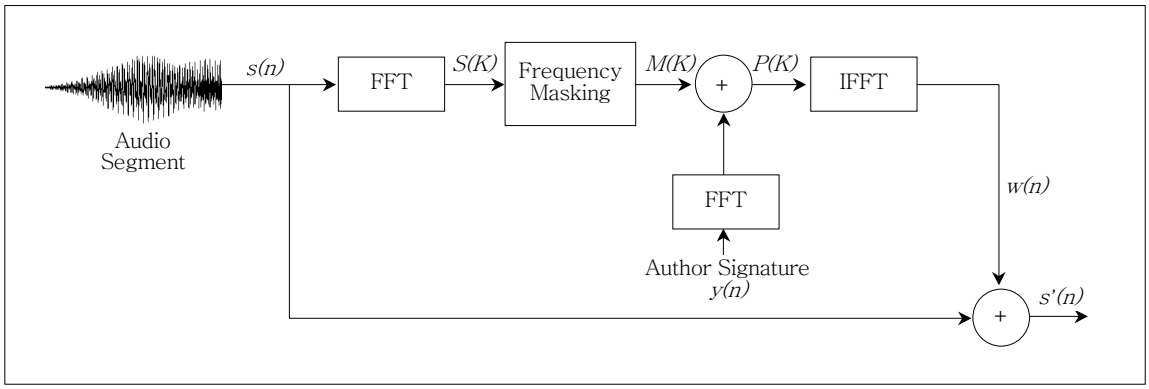
(d) Gaussian noise + lowpass filtering
similarity: 21.70
correlation coefficient: 0.7112

(그림 4) 워터마크가 내장된 영상 및 공격이 가해진 경우의 워터마크 검출 예

후 저대역통과필터를 거친 경우를 보여주고 있다. 공격이 가해진 영상에서 워터마크 알고리즘이 얼마나 강인한가를 판별하는 척도는 유사도와 상관계수의 값이 얼마나 크게 나왔느냐에 달려있다.

VI. 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. 본 장에서는 최근까지 연구된 오디오 데이터 워터마킹 방식 중 공격에 강하면서도 상대적으로 오디오의 품질을 손상시키지 않는 것으로 알려진 Swanson의 방식을 소개한다[15]. 이 방법은 인간의 청각특성을 이용하는 방법으로써 MPEG 오디오의 심리음향 모델 1을 이용하는 방법이다. 이 방식은 삽입될 워터마크를 발생시킨 뒤 발생된 워터마크를 청각특성을 고려한 심리음향 모델 1을 이용한 마스킹 곡선과 곱해서 원래의 스펙트럼에 더 해주게 된다. 즉, 마스킹



(그림 5) Swanson 방식에 의한 오디오 데이터 워터마킹 과정

곡선을 이용함으로써 워터마크가 삽입된 후에도 오디오 데이터의 품질을 떨어뜨리지 않게 되며 임의의 공격에도 강인한 특성을 지니게 된다. 전체적인 알고리즘은 다음과 같다.

- 오디오 신호를 일정크기의 처리 단위인 프레임으로 나눈다.
- 프레임 단위의 오디오 데이터의 전력 스펙트럼을 구한다.
- 구해진 스펙트럼에서 순음 성분과 잡음 성분을 구한다.
- 가청한계곡선 이하의 성분을 제거한다.
- 각각의 순음 성분과 잡음 성분에 대한 마스킹 곡선을 구한다.
- 구해진 각각의 마스킹 한계치를 이용하여 전체적인 마스킹 곡선를 구한다.
- 프레임 길이와 동일한 랜덤신호를 발생시킨 후 전력 스펙트럼을 구한다음 미리 구해진 오디오 신호의 마스킹 곡선과 곱한 다음 역변환하여 시간영역의 워터마크를 구한다.
- 구해진 워터마크를 오디오 신호에 더하여 삽입한다.

(그림 5)는 Swanson이 제안한 방식에 대한 전체적인 워터마킹 과정을 나타내고 있다. 이 방법에서 워터마크의 검출과정은 앞 장에서 설명한 Cox의 방법과 동일하다. Swanson의 방식 역시 워터마크 검출 시 원래의 데이터가 필요하다는 단점을 가지고 있다.

Ⅶ. 결 론

본 고에서는 멀티미디어 데이터의 소유권을 보호할 수 있는 워터마킹 기술의 역사와 정의 및 응용범위, 워터마크가 갖추어야 할 조건들, 그리고 문자, 영상 및 오디오 데이터의 워터마킹 기술에 대해 살펴보았다. 워터마킹 기술은 멀티미디어의 저작권 문제가 크게 대두되면서 많은 관심을 끌고 있다. 워터마킹 기술은 키를 알지 못하면 컨텐츠를 전혀 알 수 없는 암호화 기술과는 달리 키를 알지 못하더라도 그 컨텐츠를 사용할 수 있으나 그 컨텐츠의 조작이나 왜곡을 통해서도 삽입된 워터마크가 제거되지 않음으로써 저작권자가 언제든지 그 컨텐츠에 대한 권리를 주장할 수 있다. 즉, 저작권자는 자신의 권리 보호를 위해 자신의 컨텐츠를 찾고 불법으로 사용되었을 경우 자신의 권리를 주장할 수 있는 최후의 정보보호 방어선을 구축하게 되는 것이다.

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.

참 고 문 헌

[1] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proc. of the IEEE*, Vol. 87, No. 7, July 1999, pp. 1079 – 1107.

[2] A. Tirkel *et al.*, "Electronic Water Mark," in *Proc. DICTA 1993*, Dec. 1993, pp. 666 – 672.

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

[4] M.D. Swanson *et al.*, "Transparent Robust Image Watermarking," *Proc. ICIP'96*, Vol. 3, 1996, pp. 211 – 214.

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

[6] W. Zeng and B. Liu, "On Resolving Rightful Ownership of Digital Images by Invisible Watermarks," *Proc. ICIP'97*, Vol. 1, 1997, pp. 552 – 555.

[7] K. Ratakonda *et al.*, "Digital Image Watermarking : Issues in Resolving Rightful Ownership," *Proc. ICIP'98*, 1998, pp. 414 – 418.

[8] M. Barni *et al.*, "DCT-domain System for Robust Image Watermarking," *Signal Processing*, Vol. 66, No. 3, May 1998, pp. 357 – 372.

[9] I. Pitas, "A Method for Signature Casting on Digital Images," *Proc. ICIP'96*, Vol. 3, 1996, pp. 215 – 218.

[10] A. Piva *et al.*, "DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image," *Proc. ICIP'97*, Vol. 1, 1997, pp. 520 – 523.

[11] J.J.O. Ruanaidh *et al.*, "Phase Watermarking of Digital Images," *Proc. ICIP'96*, Vol. 3, 1996, pp. 239 – 242.

[12] J. Brassil *et al.*, "Electronic Marking and Identification Techniques to Discourage Document Copying," *IEEE J. Select. Areas Commun.*, Vol. 13, Oct. 1995, pp. 1495 – 1504.

[13] I. Cox *et al.*, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. on Image Processing*, Vol. 6, No. 12, Dec. 1997, pp. 1673 – 1687.

[14] W. Bender *et al.*, "Techniques for Data Hiding," *IBM System Journal*, Vol. 35, 1996, pp. 313 – 336.

[15] M. Swanson *et al.*, "Robust Audio Watermarking using Perceptual Masking," *Signal Processing*, Vol. 66, No. 3, May 1998, pp. 337 – 355.