

# 멀티미디어 시스템에서 영상 보호를 위한 워터마킹 기술에 관한 연구

이윤식\*, 최성진\*\*

한국방송공사 방송망운영국\*, 서울산업대학교 매체공학과\*\*

## Abstract

21세기 정보화사회에서 네트워크화된 멀티미디어 시스템의 증가는 디지털 정지영상과 비디오의 저작권 보호의 필요성을 대두시키고 있다. 저작권 보호는 영상 콘텐츠의 소유권 인증 및 영상의 불법적 복사물들의 식별을 위해 필요하다.

이것을 위한 하나의 접근방법이 영상에 디지털 워터마크로 알려진 보이지 않는 영상 정보를 삽입함으로써 영상을 마크하는 것이다. 디지털 워터마킹은 지금까지 공간 영역(spatial domain)과 주파수 영역(frequency domain)의 특성에 따라 각기 다른 방법들이 연구되어 왔다. 본 고에서는 워터마크의 정의, 조건, 응용분야들을 소개하고 현재까지 개발된 워터마크 방법들을 간략히 서술하며, 이들이 갖고 있는 문제점들을 언급한다.

## 1. 서론

최근 디지털 미디어의 보편화와 방송, 인터넷, 전자출판산업 등의 급격하고 광범위한 성장으로 다양한 멀티미디어 콘텐츠들이 데이터베이스화됨으로써 영상, 음성, 사진 등이 상호 공유되어 다양한 방법으로 저장, 접근이 가능해졌다. 자신이 만들어낸 디지털 멀티미디어 창작물에 대해 불법적인 사용과 인위적인 조작 등으로부터 저작권을 효과적으로 보호하기 위한 방법들이 나타나고 있는데, 이중 하나가 디지털 워터마킹기술이다 [1]. 전통적으로 저작권 증명을 위한 방법으로 화가들은 그림에 서명을 하였고, 각종 증명서에는 도장을 찍고, 지폐에는 초상화를 넣었는데, 이러한 종류들은 오래 전부터 원본 문서 또는 그림의 저작자를 나타내기 위하여 사용되어 왔다. 그러나 디지털 세상에서는 눈으로는 진짜를 구별하기 어려운 모조 영상들이 디지털 기술로 만들어 질 수 있게 되었다. "눈으로 보는 것이 믿는 것이다."라는 말은 이제 옛말이 되어 버렸다. 전통

적인 워터마킹 방법은 복제시 워터마크가 제외되어야만 된다는 특징을 갖는 반면, 디지털 워터마킹은 멀티미디어 콘텐츠에 삽입한 사용자 정보인 디지털 워터마크가 불법 복제 및 변형 후에도 존재하여 차후에 멀티미디어 콘텐츠에 관한 법적인 문제가 발생하였을 경우 워터마크를 추출하여 저작자의 소유권한을 확인할 수 있도록 하는 기술이다.

사전적인 의미로 워터마크란 「투명한 이미지」를 의미하고, 이렇게 인간의 시각 시스템으로는 드러나지 않게 표시를 해 두는 일련의 과정들을 워터마킹이라고 한다. 예를 들어 어떤 미술작품이나 책의 저자 또는 저작권을 갖고 있는 사람이 자신의 것이라는 것을 표시하기 위해 특별한 방식으로만 볼 수 있는 약품 등으로 실제 작품에 표시해 두는 것이다. 이런 워터마킹 기법을 그대로 컴퓨터에 적용한 것이 바로 「디지털 워터마킹」이다. 디지털 워터마킹의 대상은 고미술품이 아닌 비디오나 오디오 같은 멀티미디어 파일, 영상 파일 등이다. 그렇다고 파일에 물이나 약품을 묻히는 것은 아니다. 어떤 숨겨진 메시지를 파일에 넣어 두는 것이다. 이 메시지는 워터마킹할 대상, 즉 사진이나 비디오 또는 오디오 파일 안에 포함시키는데 단지 파일 뒤에 특정 값만 첨가되는 것이 아니라, 파일의 내용 안에 뒤섞이게 된다. 따라서 원래 파일보다 크기가 커지지 않으며 원래의 파일 포맷이 아닌 새로운 형태로 저장되는 것도 아니다. 또한 이렇게 워터마킹된 파일은 보통방식으로는 절대로 이 파일 안에 워터마킹 데이터가 숨겨져 있는지 알 방법이 없다. 그야말로 감쪽같이 숨겨지게 되는데 숨겨진 워터마크를 읽어내기 위해서는 특별한 소프트웨어가 필요하다. 즉, 컴퓨터분야에서 사용한 복제방지 기술은 흐린 바탕무늬 또는 로고 등을 디지털 영상 원본에 삽입해 사용자가 영상을 보거나 소프트웨어를 사용하는데 지장을 주지 않으면서도 복제를 방지하는 독특한 기술이다. 이 기술은 디지털 신문과 잡지, 디지털 도서관, 전자 박물관, 주문형 비디오, 주문형 오디오, 웹 TV와 디지털 라디오의 프로그램(드라

마, 음악, 특집물) 등의 제품과 공문서의 인증 기능 등에 사용될 수 있기 때문에 최근 선진국에서는 빠르게 연구가 확산되고 있다. 디지털 정보는 변형조작이 쉬워 인터넷에서의 콘텐츠 보호차원에서 복제로 인한 소유권 문제 해결을 위해 효율적인 보호기술이 요구되고 있다. 일반적인 저작권법으로는 디지털 속성을 이용한 저작권을 보호하는 것은 사실상 어렵다. 디지털로 생성된 원본이 복사를 통해서 온라인 상으로 배포될 때 이 작품의 주인이 과연 누구인가에 대한 분쟁이 발생하게 된다. 따라서, 이 원본의 소유주임을 확실히 증명할 수 있다면 이 분쟁은 간단히 해결될 것이며, 또한 불법유통을 미연에 차단할 수 있을 것이다. 이 기술은 원본의 출처를 밝히거나 누구에게 전달된 정보인지 추적하는 데도 쓰이며, 한마디로 원천적인 복제방지보다 복제경로를 찾아내는 저작권 보호기술에 가깝다.

디지털 영상물에 대한 저작권 보호를 위해 기존에 이용된 여러 가지 방법들을 살펴보면 다음과 같이 분류할 수 있다[2].

첫째, 네트워크 접근을 통제하는 방화벽(firewall)을 구축하여 영상을 보호하는 것이다. 그러나 이 방법은 일단 사용자 인증이 승인된 후 사용자 임의의 자료 배포는 막을 수 없다.

둘째, 공용키(public key) 암호화 알고리즘을 이용하여 암호화하고 개인키(private key)를 이용하여 영상물을 원래의 데이터로 복구해 내는 방법이다. 이 역시 개인키로 암호화 한 후 배포하는 것에는 무방비하게 된다.

셋째, 영상물의 불법적인 조작을 막고 영상의 소유권을 보장할 수 있는 디지털 워터마크(watermark) 방

법이 있다. 앞의 두 방법과 더불어 부가적인 기능으로 사용자 정보, 저작권 정보, 배포자 정보 등을 삽입함으로써 법적인 분쟁이 발생하였을 때 해결책을 제시할 수 있다. 이와 같이 정보를 은닉하고 보호하기 위해 연구 개발된 것들은 그림 1-1과 같이 분류 정리될 수 있고, 1999까지 공식적으로 발표된 관련 연구의 수는 표 1-1과 같다.

표 1-1 디지털 워터마크 발행 수

년	1992	1993	1994	1995	1996	1997	1998
발행수	2	2	4	13	20	64	103

본 고의 구성은 다음과 같다. II장에서는 워터마크의 정의, 특성 및 워터마크가 다른 응용분야에서 필요로 하는 요구사항들을 살펴보고, III장에서는 워터마크의 관련연구들에 대해서 간략히 살펴본다.

## II 워터마크의 조건과 응용

본 장에서는 워터마크의 정의, 특징 및 원리 등 워터마크가 갖춰야 할 조건들과 응용분야들을 살펴본다.

### 2.1 워터마크의 정의

디지털 워터마크란 디지털 콘텐츠에 사용자의 ID나 자신만의 정보를 삽입시켜 놓으므로써 불법적인 복제를 막고 데이터 소유자의 저작권과 소유권을 효율적으

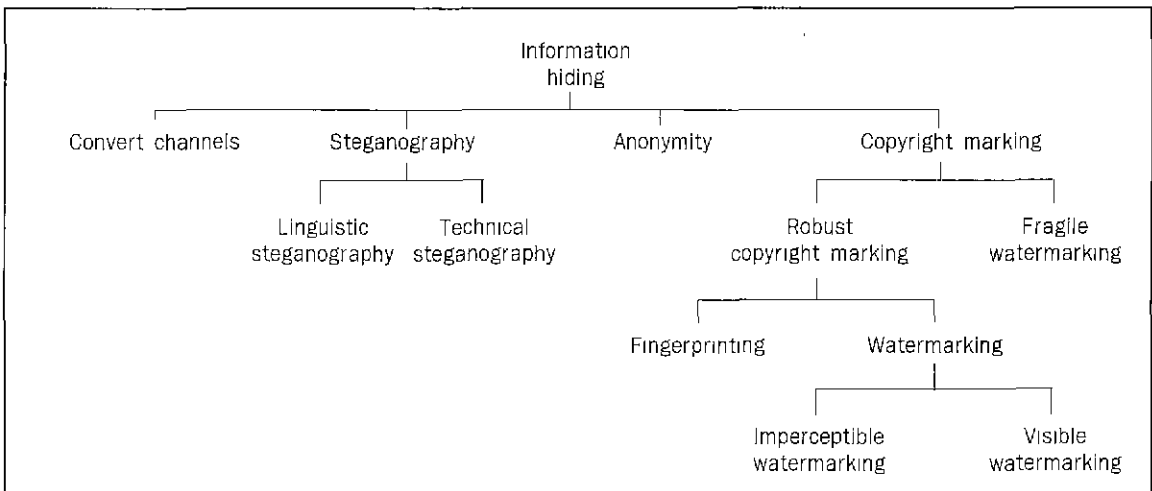


그림 1-1. 정보 은닉 기술의 분류

로 보호하기 위한 방법으로써 데이터에 일정한 암호를 숨겨서 부호화하는 과정이며, 이러한 부호를 워터마크라 하며, 영상이나 음성 등에 특정한 코드나 패턴 등을 삽입하는 기술이다. 또는 어떤 미술품이나 책의 저자나 주인이 이 작품이 자신의 것임을 표시하기 위해 육안으로 보이지 않는 특수한 형태의 표시를 해두는 것을 말하며, 물이나 특별한 방식으로만 볼 수 있는 약품으로 실제 작품에 표시해두는 것으로 정의되고 있다. 결국 디지털 워터마크는 디지털 정보나 기존의 아날로그 형태의 정보를 디지털화 할 때, 첨가시키는 일종의 저작권관리 정보로서 개인의 식별기호나 부호를 삽입하는 표시라고 정의 내려질 수 있을 것이다.

## 2.2 디지털 워터마킹의 원리

디지털 워터마킹은 원래의 멀티미디어 데이터에 일정한 신호를 포함시키는 기법이다. 이를 수학적으로 설명하면 다음과 같다. 워터마킹을 할 대상으로 하나의 영상이 있다고 가정해 보자. 어떤 영상  $I$  가 있을 때, 디지털 워터마킹 작업은  $I$  에 우리가 넣고자 하는 정보  $w$ , 그리고 원 영상  $I$  를 인자로 하는 함수 값, 즉  $f(I, w)$  를 원래의 영상  $I$  에 추가하는 작업이라고 할 수 있다.[5] 이때 워터마킹된 영상  $I'$  는 식(2-1)과 같이 표현된다.

$$I' = I + f(I, w) \quad (2-1)$$

만약 워터마킹 신호를 원래의 영상과는 별개로 만들려고 한다면, 워터마크 신호  $f$  는  $f(w)$  가 될 수 있다. 이때는 워터마킹할 정보  $w$  외에는 워터마크를 만들 것이 없으므로  $w$  를 워터마크 영상으로 사용할 수도 있을 것이다. 이때는 식(2-2)와 같이 된다.

$$I' = I + f(w) = I + w \quad (2-2)$$

워터마킹된 영상  $I'$  는 여러 곳을 거치면서 내용의 일부가 변경되거나 깨지는 상황을 맞을 수 있다. 이때 이를 유발하는 작업을  $n$  이라고 하자. 그런데 이 작업  $n$  은 일반적으로 원 영상에 따라 결과가 좌우되는 경우가 많다(그렇지 않은 작업도 있지만, 개념을 위해  $n$  에 제한을 두자). 따라서  $n$  은 영상  $I$  를 인자로 하는 함수  $n(I)$  로 생각할 수 있다. 따라서 워터마킹된 영상을 디스플레이 프로그램으로 보려고 할 때, 보고자 하는 영상은  $I'$  가 작업  $n$  에 의해 약간은 다른 영상  $I''$  가 될 것이라 생각할 수 있다. 즉,

$$I'' = I' + n = I + f(I, w) + n(I) \quad (2-3)$$

많은 디지털 워터마킹 방법들은 기본적으로 위와 같은 수식을 기본 개념으로 원 영상에 워터마킹을 하여 새로운 영상을 만들어 내는 방식을 택하고 있다. 이 방법들은 크게 다음 두 가지의 상황을 고려하고 있다.

원 영상과는 무관하게 워터마킹 신호를 만드는 경우 ( $I' = I + w$ )와 워터마킹 시킬 정보와 원래의 영상을 가지고 만드는 경우 ( $I' = I + f(I, w)$ )의 두 가지 방법이 있다. 첫 번째 경우, 원래의 영상과는 무관하게 워터마킹 신호를 만들 경우에는 워터마크 정보를 시각필터링을 거쳐서 원래의 영상 안에 은닉시킬 수 있는 형태로 만든 다음 원 영상과 결합해 워터마킹된 영상을 만들게 된다. 두 번째 경우, 원 영상과 워터마킹 정보를 결합해 워터마킹 신호를 만들 경우에는 시각필터링을 거쳐서 나온 신호와 원 영상을 비선형 결합시켜 원래의 영상에 워터마킹을 취하는 형태가 된다.

한편, 콕스(Cox)[6]는 논문에서 워터마킹 신호에 가중치  $a$ 를 두어서 워터마킹을 수행하는 방법을 제시했다. 이것은 식(2-4)와 같이 표현된다.

$$I' = I (1 + aw) \quad (2-4)$$

콕스 방법의 장점은 영상이 특정한 주파수 채널에서 해상도나 선명도가 강조되거나 줄어들 때, 그에 따라서 워터마킹 정보도 같이 비중이 변할 수 있다는 점이다. 이상의 방법들을 기초로 해 많은 워터마킹 기법들이 다양한 멀티미디어 데이터에 적용되었다. 텍스트에 워터마킹을 하는 법, 콤팩트 디스크의 내용 안에 워터마크를 추가하는 법 등 다양한 방법들이 제시되었다. 위의 방법론적인 결과로 다음과 같이 워터마크 삽입과정을 요약 할 수 있다.

아날로그 신호를  $I$  라 할 때  $I$  를 샘플링하여 디지털 신호  $D$  를 구할 수 있다. 디지털 신호로부터 워터마크를 삽입할 수 있는 형태로 변환된 데이터를  $V$ , 삽입하고자 하는 정보를  $W$ ,  $W$  가  $V$  에 삽입될 수 있도록 변환된 정보를  $X$  라고 가정한다.  $X$  가 삽입되면  $V'$  를 얻을 수 있고,  $V'$  로부터  $D'$  를 추출을 하고  $D'$  를 다시 샘플링을 하여  $S'$  를 구할 수 있다. 여기서  $D'$  가 워터마크가 삽입된 자료라고 볼 수 있다. 일반적인 워터마크 삽입 과정은 그림 2-1과 같다.

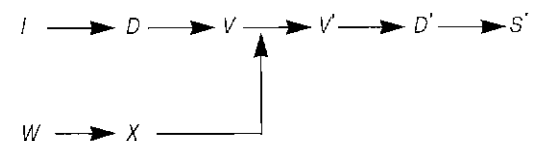


그림 2-1. 일반적인 워터마크 삽입 과정

### 2.3 워터마킹의 목적

워터마크 방법은 다양한 목적으로 사용될 수 있다. 다음은 워터마크를 사용하는 여러 가지 용도를 보여준다[2][4].

#### 2.3.1 소유권 증명(ownership assertion)

이것은 디지털 미디어 콘텐츠의 소유관계를 주장하는 방법으로 워터마크를 사용하는 것이다. 콘텐츠에 대한 소유를 주장하기 위해서, 먼저 콘텐츠를 만드는 작가는 비밀키(private key)를 사용해서 워터마크를 생성한 뒤, 그것을 원본 콘텐츠에 삽입을 한다. 이후 작가는 워터마크가 삽입된 영상을 공개한다. 나중에 다른 사람이 이 공개된 콘텐츠의 소유를 주장하면 원래 콘텐츠를 생성한 작가는 워터마크가 없는 원본 콘텐츠를 생성해서 소유를 주장하는 다른 사람의 영상에 자신이 삽입한 워터마크가 있음을 보여 주면 되는 것이다. 이때 작가의 원본 콘텐츠는 소유를 주장하는 다른 사람에게는 알려지지 않았으므로 다른 사람은 작가처럼 자신의 소유를 주장할 수 없게 된다. 하지만 이런 방법이 동작하기 위해서는 영상에 대한 압축, 확대, 축소 등과 같은 연산을 수행해도 워터마크가 없어지지 않고 남아 있어야 한다.

#### 2.3.2 인증 및 무결성 확인(authentication and integrity verification)

이것은 멀티미디어 콘텐츠가 법적인 용도, 의학적인 용도, 뉴스 또는 상업적인 용도로 사용되는 경우에 콘텐츠를 만든 창작자가 누구인지 확인함과 동시에 그 미디어가 훼손되거나 수정되지 않았다는 것을 확인하는 것이다. 일반적인 인증은 암호학적인 방법을 사용해서 해결할 수 있다. 하지만 워터마킹 방법을 사용하면 콘텐츠에 대한 인증을 수행하는 부분이 콘텐츠에 포함되어 데이터를 처리하는 문제를 간단히 할 수 있게 된다. 이 방법이 동작하려면 영상의 변경에 대해서 확인 가능한 장치가 있어야 한다. 즉 데이터에 대한 인증과 무결성(integrity)의 목적은 콘텐츠의 창작자를 확인함과 동시에 콘텐츠의 내용이 변경되거나 훼손되지 않았다는 것을 확인하는 것이다. 또한 콘텐츠에 수정이 일어난 경우 어느 위치에 수정이 발생했는지 확인하는 것이 필요하다. 영상에 대한 인증과 무결성을 보장하기 위한 방법은 기존에 여러 가지가 있다.

#### 2.3.3 지문(fingerprinting)

본 방법은 디지털 미디어의 무단 복제와 무단 배포를 막기 위한 방법이다. 먼저 콘텐츠의 저자는 각각의 데이터 복사본에 대해서 유일한 워터마크 즉, 지문을

부여해서 그 데이터 복사본에 삽입을 한다. 만일 무단으로 복사된 콘텐츠가 발견되면 복사본 내에 숨겨져 있던 지문은 변하지 않았으므로 복사본의 원본이 어떤 것인지를 알아내어 불법 복사를 한 사람을 찾아 낼 수 있게 된다. 본 방법이 동작하려면 워터마크를 삭제하려 하거나 워터마크가 동작하지 못하도록 하려는 여러 가지 시도에 대해서 안전해야만 한다.

#### 2.3.4 콘텐츠 레이블(content labeling)

이것은 워터마크를 사용해서 콘텐츠에 대한 추가적인 정보를 제공하는 것이다. 한 예로 영상을 만드는 경우 이 영상이 만들어진 시간, 창작자등과 같은 정보를 워터마크로 만들어서 이미지에 삽입하는 것이다.

#### 2.3.5 사용 횟수 조절(usage control)

이것은 멀티미디어 콘텐츠를 복사하거나 재생하는데 특별한 하드웨어 장치가 필요한 경우, 디지털 워터마크가 콘텐츠에 삽입되어 콘텐츠를 복사할 수 있는 횟수 등을 제어하는데 워터마크를 사용하는 것이다. 이 방법의 경우 매번 복사가 일어날 때마다 하드웨어가 워터마크를 수정하게 되므로 나중에는 더 이상 복사되지 않게 될 것이다. 앞에 나타난 바와 같이 각각의 워터마킹 방법은 그것이 사용되는 용도에 따라서 서로 다른 요구조건을 지니고 있다. 그리고 이런 다양한 요구조건을 모두 만족하는 워터마킹 방법은 아직 존재하지 않고, 이런 조건들을 모두 만족시키는 워터마킹 방법을 만드는 것은 아주 어렵다.

### 2.4 디지털 워터마킹의 특징

디지털 워터마킹은 다양한 특징들을 구비하여야 한다. 왜냐하면 저작권 관리정보의 파손을 불법적인 접근자나 획득자가 시도할 것이 분명하기 때문이다. 즉, 불법적인 획득은 실질적으로 그 내용정보를 확인하더라도, 내용에 대한 파악이 어렵기 때문에 실질적으로 활용하기에는 부적절할 수도 있기 때문이다. 앞서 고찰한 대로, 암호화를 위한 기존의 방법으로는 암호화 기법(encryption)이 있다. 그러나 워터마크는 기존의 암호가 해독되지 않으면 콘텐츠를 볼 수 없고, 또 일단 한번 해킹되어도 원래의 콘텐츠는 동일하며, 다르게 워터마킹 된 후에도 외관상으로는 원래의 콘텐츠와 거의 차이가 없고, 삽입된 워터마크는 콘텐츠에 변형을 가해도 쉽게 없어지지 않는 특징이 있다.

디지털 워터마킹 기법에는 식별/인식 가능한 것과 식별/인식이 불가능한 것의 두 가지가 있는데, 전자는 특별히 소유권에 대한 빠른 주장이 가능하다는 점에서 유용하며, 후자는 권리의 보호 측면에서 강하게 입증할 수 있다는 특징을 지닌다. 그리고 디지털 워터마킹 기

술이 적절하게 의도된다면, 소유권의 증거로서, 내용인 증 도구로서, 그리고 데이터에 삽입하는 지문장치의 수단으로서 데이터의 부적절한 사용에 대한 추적도 가능하게 할 것이다[8]. 그리고 디지털 워터마킹이 효과적으로 적용하기 위해서는 다음 요건들을 만족시켜야 한다.

#### 2.4.1 알아보기가 어려워야 함(difficult to notice)

일단 가장 중요한 사항으로, 디지털 워터마킹이 원래의 데이터에 포함되었는지를 쉽게 알아볼 수 없도록 워터마킹이 구현되어야 한다. 또한 워터마킹이 포함됨으로 인해 원래 데이터의 품질에 이상이 생기는 일이 없어야 한다. 이에 대해서는 아직도 기술적으로 해결해야 할 사항들이 많다. 예를 들면, 최근의 멀티미디어 데이터들은 JPEG, MPEG처럼 어느 정도의 손실을 감수한 압축기법이 사용되는 경우가 많다. 이때, 워터마킹이 된 원래의 데이터를 손실 압축했을 때 워터마킹이 그대로 유지가 될 수 있는지, 그리고 원래 데이터의 품질이 그대로 유지가 될 수 있는지의 여부가 중요한 논의 대상이 될 수 있다. 이러한 요구사항을 만족하기 위하여 인간이 신호의 변화를 인식하지 못하는 휘도(luminance) 평면의 DCT주파수 계수값(JND : Just Noticeable Difference)을 구하는 워스톤(Watson)과 솔로몬(Solomon)의 시각 시스템 모델을 사용한다[9].

#### 2.4.2 신호의 일반적인 일그러짐에 대해 강인성이 유지되어야 함(robustness)

디지털 형태의 음악, 사진, 비디오 신호들은 일반적으로 다양한 형태의 일그러짐이 있다. 그리고 JPEG나 MPEG에서의 손실 압축의 경우, 신호의 중요하지 않은 부분의 정보는 사라지기 때문에 중요하지 않은 영역에 삽입된 워터마크는 제거될 확률이 있다. 또한 멀티미디어 데이터들은 많은 손실 요소인 필터링, 압축, 밝기조정(contrast enhancement), 잘라내기(cropping), 회전 등으로 인해 원래의 데이터에서 신호들이 일그러질 수 있는 경우를 많이 포함하고 있다. 이러한 다양한 신호의 손상에도 불구하고 워터마크는 추출이 되어야 한다[6]. 영상의 선명도를 높인다거나, 색상의 일부를 바꾼다거나, 또는 오디오 신호의 기저주파수를 증폭시킨다거나 할 때, 데이터 안에 있는 워터마킹이 깨지지 않고 유지될 수 있는가, 또한 워터마크를 읽을 수 있는 디스플레이가 이렇게 변경된 데이터 안에 있는 워터마크를 읽어낼 수 있는가가 워터마킹의 중요한 문제가 될 수 있다.

#### 2.4.3 워터마크를 없애기 위한 시도에 대처할 수 있어야 함(tamper-resistance)

멀티미디어 데이터에 워터마크가 포함되어 있다는 사실을 안다면 워터마크를 없애기 위한 시도가 분명 존재할 수 있다. 또한 같은 데이터에 여러 다른 워터마크가 각각 포함되었을 때(한 멀티미디어 데이터를 여러 사람들이 구입할 때, 각각 다른 워터마크를 부여할 수 있을 것이다. 이때 이런 상황이 발생한다), 이들 간의 차이점을 비교해 워터마크 신호를 찾아서 없애려는 시도가 있을 수 있다. 이때 이를 방지할 수 있는 매커니즘이 있어야 할 것이다.

#### 2.4.4 응용 프로그램을 위한 적당한 데이터율(bit rate)

워터마크 신호 안에 포함될 수 있는 정보의 양도 워터마킹에서 중요한 이슈가 된다. 워터마크를 필요로 하는 환경에 따라서 삽입될 정보는 미리 정해진다. 영상에 대해서 일반적으로 300~400[bit] 정도의 정보를 삽입한다. 어떤 경우여라도 시스템 설계자는 자료에 숨겨질 비트(bit)의 수를 고려하여야 한다.

#### 2.4.5 낮은 에러 확률을 가져야 함(low error probability)

고의적이거나 비고의적인 훼손과 손상이 없더라도 워터마크를 추출하는데 실패할 확률과 워터마크가 존재하지 않는데 존재할 확률이 아주 작아야 한다. 종종 통계학에 기반한 알고리즘은 이와 같은 요구조건을 만족한다. 워터마크가 법적인 신뢰성을 증명하기 위해서 이와 같은 요구조건을 보여줄 수 있어야 한다.

#### 2.4.6 워터마크를 변경하거나 계속 추가할 수 있어야 함(modification & multiple watermarks)

어떤 경우에는 워터마크가 포함된 이후에 워터마크의 내용을 변경할 필요가 있다. 이때 기존의 워터마크를 없애고 새 워터마크를 추가하거나, 또는 기존의 워터마크 외에 새로운 워터마크를 계속해서 추가하는 방법을 생각할 수 있다. 또한 멀티미디어 데이터의 배포가 여러 단계를 거쳐갈 때 각각 워터마크를 추가해 원래의 데이터가 어떤 경로를 거쳐 배포가 되었는지를 파악하게 할 수 있을 것이다. 이 점에 대해서도 고려할 것들이 많이 있다.

#### 2.4.7 워터마크의 확장이 용이해야 함

어떤 암호를 풀어내는데 현재의 컴퓨터 능력으로는 거의 불가능할 정도로 오랜 시간이 필요하다고 해서 이 암호가 영원히 깨지지 말라는 법은 없다. 요즘 언급되고 있는 바이트 코드들 예로 들 수 있을 것이다. 성서 문구 안에 있는 단어들을 찾기 위해 몇 천개의 연산이 빨리 이루어져야 했고, 뉴턴 시대에는 이것이 불

가능하였지만, 최근의 컴퓨터 기술의 발전으로 인해 이러한 연산을 쉽게 수행할 수 있었다. 이렇게 현재의 기술로 알아보기 힘들게 만든 워터마킹이 이후 더 강력한 컴퓨터와 훌륭한 알고리즘이 개발되었을 때는 쉽게 깨질 수 있는 상황이 발생할 수 있다. 이때 다시 새로운 워터마킹 알고리즘을 만들어 기존 것을 대체할 것이 아니라 기존의 워터마크를 확장함으로 더욱 강력한 워터마킹을 수행할 수 있게 하면 어떨까? 이점도 워터마킹과 관련해서 논의 가치가 있는 내용이다.

#### 2.4.8 원본을 사용하지 않고 워터마크 추출을 할 수 있어야 함

자료들로부터 숨겨진 정보를 정확하게 추출하기 위하여 복잡한 알고리즘이 사용된다. 신뢰할 만한 알고리즘을 개발하기 위하여 워터마크가 삽입된 자료와 삽입되지 않은 원본을 이용하여 추출을 하기도 한다. 하지만 실제세계에서는 원본 없이 추출해야 하는 경우도 상당수 발생할 수 있다.

### III 워터마크의 관련 연구

영상은 디지털 워터마킹으로 알려진 방법에 의해서 인증되어질 수 있다. 워터마크는 앞에서 언급했듯이 암호 코드 또는 소유자와 영상의 콘텐츠 둘 모두의 증명을 위해 원 영상속에 포함되는 영상이다. 지각적으로 인식할 수 없는 워터마크들의 사용은 영상 인증의 한 형태이다. 워터마킹 알고리즘은 세 부분으로 구성된다.

1. 워터마크
2. 마킹(marking) 알고리즘
3. 증명(verification) 알고리즘

첫 번째 워터마크는 각각의 소유자가 갖는 독특한 워터마크를 의미한다. 마킹 알고리즘은 영상안에 워터마크를 삽입하는 과정 및 방법을 의미하고, 증명 알고리즘은 소유자와 영상의 무결성 둘 모두를 결정하기 위해 삽입된 워터마크를 인증하는 과정을 의미한다.

초기의 워터마킹 방법들 중 하나는 영상 데이터의 체크섬(checksum)을 구한 후 무작위로 추출된 픽셀들의 LSB 안에 체크섬을 삽입하는 것이다. 다른 방법들은 수정된 최대 길이 선형 이동 레지스터 시퀀스를 화소 데이터에 추가하는 것이다. 이들은 수정된 시퀀스와 워터마크된 영상과의 공간 교차상호관계 함수를 사용하여 워터마크를 확인한다. 또한 워터마크들은 직접적으로 영상의 공간 혹은 변환계수들을 수정할 수 있다. 이것들의 알고리즘들은 소유자에게만 알려진 시퀀스에 의해 DCT 계수들을 변조한다. 워터마킹 기술들은 영상에 의존될 수도 있다. 이러한 기술들은 마크를 지각할

수 없도록 하면서 동시에 영상내의 워터마크의 레벨을 증가시킨다. 어쨌든 디지털 워터마킹은 공간 영역적 방법과 주파수 영역적 방법으로 대별될 수 있다. 이에 대한 기술들의 특징을 간략히 살펴본다.

#### 3.1 공간 영역의 디지털 워터마크

먼저 물리적 화소영역, 즉 공간 영역에서의 워터마크를 삽입하는 방법 중 가장 간단한 방법으로는 각 화소에서의 그레이 레벨(gray-level) 값의 LSB(least significant bit)를 발생된 난수에 의해 바꿈으로써 영상 공간 내 밝기 값의 LSB에 서명 문양을 숨기는 방법이 있다. 그러나 이 간단한 방법은 워터마크가 찍힌 영상에 대한 압축손실, 전송에러, 편집 및 특수 처리 등에 매우 약하다는 단점을 갖고 있다. 이 단점을 극복하기 위해 인간의 시각 특성을 이용한 마스킹 효과에 의해 영상 내에 텍스처 영역이나 윤곽선 둘레의 밝기 값의 변화를 육안으로 잘 구별할 수 없다는 점을 이용하여 그 부분에 대해 영상 밝기 값을 특별히 더 많이 변화시킴으로써 워터마크 검출시 신뢰도를 높이는 방법이 있다.

#### 3.2 주파수 영역의 디지털 워터마크

영상 데이터를 DCT, DFT, DWT 등과 같은 변환으로 주파수 공간으로 변환하여 그 주파수 영역들 중에서 시간적으로 덜 민감한 성분에 적응적으로 워터마크를 삽입하는 방법이다. 단일 주파수 성분을 변화시킴으로써 변환 블록내의 밝기 값 전체에 영향을 미치고, 따라서 불법적인 공격에 강한 워터마크를 만들 수 있다. 영상 데이터를 주파수 형태로 변환했을 때 가질 수 있는 통신 채널이라고 가정하면 워터마크는 그 통신 채널로 통과하는 신호라고 볼 수 있다. 그 신호가 잡음, 필터링, 압축전송 등에 영향을 받지 않고 효과적으로 전송이 될 수 있도록 대역확산통신(spread spectrum communication) 방식을 도입한다[1]. 특정 주파수 대역의 에너지는 감지할 수 없을 정도로 작지만 주파수의 위치와 변화량을 알고 있는 소유권자에 의해 산재해 있는 주파수 성분을 모으면 높은 신호 대 잡음비로 신호를 검출할 수 있다. 워터마크 신호를 영상(전송채널)이 갖고 있는 여러 주파수 영역으로 확산시킴으로써 특정 주파수 대역의 에너지를 감지하기 어렵게 한다. 이런 방식의 단점으로는 전 주파수 영역을 골고루 쓰다 보면 일반적인 신호처리 등을 거치게 되면서 워터마크 성분의 손실을 유발할 가능성이 많다.

이런 단점을 극복하기 위해, 영상 처리과정에서 손실되는 정보의 양을 최소한으로 줄이면서 시간적인 영상의 변화를 감지하지 못하도록 하는데 큰 장점을 갖는 방법들이 연구되고 있다. 즉, 영상의 변화를 감지 못

하면서 시각적으로 중요한 영역에 정보를 삽입하는 알고리즘을 사용함으로써, 시각적 변형과 JPEG 압축, 그 외 영상 처리기술에 대하여 장단점을 고려하여 삽입하고자 하는 주파수 영역을 선택함으로써 워터마크를 삽입하는 알고리즘이다.

### 3.3 기존에 사용된 디지털 워터마킹의 분석

공간 영역에서의 워터마킹으로는 특정 위치의 화소 밝기 정보를 진폭 변조하여 인접 화소와 비교해서 워터마크를 검출하는 Kutter 방법[11]과 칼라 영상의 공간 영역에 워터마크 패턴을 삽입하는 Hashida 방법[12] 등이 제안되었다. 이들 공간 영역에서의 워터마킹은 계산량이 비교적 적고 쉽게 워터마킹을 할 수 있지만 잡음에 워터마크가 강인하지 못하고, JPEG등과 같은 영상압축에 적용하기 어려운 단점이 있다[1].

주파수 영역에서의 워터마킹은 원 영상을 DCT 혹은 DFT, 웨이브렛 등으로 변환한 후 적당한 주파수 대역에 워터마크를 삽입하는 방법이다. 워터마크가 삽입되는 주파수 대역은 워터마킹 방법에 따라 고주파 영역, 저주파 영역 혹은 중간 주파수 영역에 워터마크를 삽입한다. Cox[1]은 영상을 DCT변환 후 시각적으로 중요한 계수를 선택하여 워터마크를 삽입하였다. 또한 Xia[13]는 영상을 웨이브렛 변환 후 최저주파 대역을 제외한 나머지 부대역(subband)에 워터마크를 삽입하였으며 영상을 다 해상도로 분해하여 단계별로 다른 가중치를 주어 워터마크를 삽입하여 성능을 향상시킬 수 있다. 그리고 Ruanaidh[15]는 주파수 영역에서 블록 별로 위상정보에 워터마킹을 하는 방법을 제안하였다. Sklar[16]은 영상 데이터를 DFT를 기반으로 주파수 변환을 하여 통신에 사용하는 대역확산통신방식 즉, m\_sequence 방식을 도입하여 여러 주파수 영역으로 확산시켜 사용자의 주파수의 위치와 변화량을 알아야 추출할 수 있는 방법을 제시하고 있다.

O' Ruanaidh and Pun[19]은 Fourier-Meln Transform을 이용하여 진폭에 워터마크를 내장하고 polar-log하여 얻어진 구 좌표계를 직각좌표계로 바꾸어 처리함으로써 공간적인 변화에 강한 방식이다. 이 방식의 단점은 푸리에변환에서 영상의 정보는 대부분 위상에 포함되어 있기 때문에 진폭에만 워터마크를 내장하는 것으로는 크기변환이나 이동에는 강인하나, 일반적인 영상처리에 강인하지 못하다는 단점을 가지고 있다.

또 다른 주파수 영역에서의 방법은 추가적인 연산이 필요하지만 압축이나 잡음에 견고한 특성을 갖는다. 그리고 대부분의 워터마킹 방법에서는 의미있는 시각정보가 포함되어 있지 않은 워터마크를 난수를 발생시켜 삽입하고 이를 검출하여 삽입전후의 상관관계를 계산

하여 소유권을 인정하는 방식이다.

위에서 언급한 방법들의 장점과 단점들을 보완한 워터마크 기술로써 대부분의 방법들이 블록 DCT를 기반으로 하고 있다. 물리적 화소영역에 대한 마스크와 주파수 영역에 대한 마스크를 두어 숨겨진 데이터의 강건성을 증가시킨다. 즉, 영상을 블록으로 나눈 다음 각각의 블록에 대하여 DCT를 행하여 인간 시각 시스템에 부합하는 주파수 영역에 대한 마스크를 적용하여 DCT인자에 의사잡음(pseudo-noise)를 삽입하고 난 후 역 DCT를 행하여 생성된 결과에 대하여 다시 물리적 영역에 대한 마스크를 적용시켜 그 변화의 여부를 거쳐 워터마크를 삽입한다. 영상을 블록으로 나누고 각 블록을 임의로 섞은 후, 이를 DCT하여 워터마크를 삽입하고 블록 안에 섞은 순서를 알지 못하면 워터마크를 검출하지 못하게 하였다.

그 외의 방법으로 wavelet 변환을 기반으로 계층적으로 워터마크를 삽입하는 방법인 DWT를 하고 난 후 부대역 고주파수 영역과 중간주파수 영역에 의사 랜덤(pseudo-random) 코드를 삽입하는 방법이 있다[13].

이러한 디지털 워터마킹 기술을 맨 처음 개발한 것은 일본의 NEC 연구소의 연구원들이다. 이들은 오디오, 이미지, 비디오를 비롯한 멀티미디어 데이터 안에 특정한 코드값을 은폐하는 방식으로 인터넷을 통해 영상과 음악의 관권에 관한 효과적인 보호 효과를 볼 수 있도록 했다. 이후 여러 군데에서 디지털 워터마킹에 관한 문서와 논문 그리고 각종 소프트웨어들을 만들었는데 그 중 주목할 만한 것들로는 디지털 워터마크(Digimarc)사의 픽처마크(Picturemarc), 시스콧(Syscop), 슈어사인(Suresign) 등이 있다.

## IV 결론

21세기 영상정보화사회가 도래함에 따라 네트워크화된 멀티미디어 시스템이 영상을 저장 관리하기 위해 급속도로 사용이 증가하고 있고, 이에 따라 디지털 미디어의 보호 필요성이 대두되고 있으며, 지적 재산권의 보호와 주장이 그 어느때보다 중요하게 되었다.

따라서 본 고에서는 최근에 영상의 보호를 위해 많이 연구되고 있는 디지털 워터마킹 기술들에 대한 개략적인 내용을 살펴보았다.

## 참 고 문 헌

- [1] I. J. Cox, J. Killian, T. Leighton and T. Shammoon, "Secure spread spectrum watermarking for

- multimedia" IEEE Trans. on Image Processing, vol. 6, no 12, pp 1673-1687, Dec, 1997
- [2] P W Wong, "A public key watermark for image verification and authentication," In Proceedings of ICIP, Oct., 1998
- [3] Fabrice A. P. Petitcolas, "Information Hiding - A Survey," Proceedings of The IEEE, vol 87, no. 7, July, 1999
- [4] P. W. Wong, "A watermark for image integrity and ownership verification," In Proceedings of IS&T PIC Conference, May, 1998
- [5] S Craver, N. Memon, N Yeo, and M. Yeung, "Can Invisible Watermarks Revolve Rightful Ownership?," IBM Research Report, RC20509, July 25, 1996
- [6] I. J. Cox, J. Klian, T. Leighton and T. Shamoon, "A Secure, Robust Watermark for Multimedia," Workshop on Information Hiding, Newton Institute, Univ of Cambridge, May, 1996
- [7] S. Walton, "Information Authentication for a Slippery New Age," Dr. Dobbs Journal, vol. 20, no 4, pp. 18-26, April, 1995
- [8] Minerva M Yeung, "Digital Watermarking," Communications of ACM, vol. 41, no 7, 1998
- [9] Andrew B Watson, "DCT Quantization Matrices Visually Optimized for Individual Image," Human Vision, Visual Processing and Digital display IV, Proc SPIE, 1993
- [10] R B Wolfgang, E. J. Delp, "A watermarking technique for digital imagery : further studies," Video and Imaging Processing Laboratory, Proceeding of the International Conf on Imaging Science, pp. 279-287, 1999
- [11] M. Kutter, J. Johnston, and R. Safranek, "Signal compression based on models of human perception," Proc. IEEE, vol 81, no 10, 1993
- [12] K I. Hashida and A. Shlozaki, "A method of embedding robust watermarks into digital color images," IEICE Trans. Fundamentals, vol. 81, no 10, Oct., 1998
- [13] X. G. Xia, C. G. Bonchelet and G R. Arce, "A multiresolution watermark for digital images," IEEE Int. Conf. on Image Processing, vol. 3, pp. 548-551, 1997
- [14] K. K. Wong C H. Tse, T H. Lee, and L. M. Cheng, "Adaptive watermarking," IEEE Trans. on Consumer Electronics, vol. 43, no. 4, pp. 1003-1009, Nov, 1997
- [15] J. O. Ruanaidh, W. J. Dowling and F M. Boland, "Phase watermarking of digital images," IEEE Proc. Int. Conf. Image Processing, vol. 3, pp. 239-242, 1996
- [16] B Skla, "Digital Communications," Prentis Hall, 1988
- [17] W B Pennebaker and J. L Mitchell, JPEG - Still Image Data Compression Standard, New York Van Nostrand Reinhold, pp. 34-38, 1993
- [18] C. J Mitchell, K Piper and P. Wild, "Digital Signatures" in Contemporary Cryptology: The Science of Information Integrity, G. J. Simmons, Editor, IEEE Press, pp 325-378, 1991.
- [19] J. J. K O' Ruanaidh, T Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking," Proceedings of ICIP' 97, Santa Barbara, CA USA, vol. I, pp. 536-539, Oct, 1997

## 필자소개



### 최성진

- 1978-1982 광운대학교 전자공학과 졸업(공학사)
- 1982-1984 : 동 대학원 전자공학과 졸업(공학석사)
- 1985-1991 동 대학원 전자공학과 졸업(공학박사)
- 1996-1997 : USM(Univ Saints Malaysia) 초빙교수
- 1999-2000 : OSU(Oklahoma State Univ.) 객원교수
- 2000-현재 . 방송위원회 기술자문위원
- 1996-현재 . 한국방송공학회 편집위원
- 1992-현재 . 서울산업대학교 매체공학과 부교수
- 주관심분야 : 디지털TV, 3DTV, 영상보호

### 이윤식

- 1994년 . 인천대학교 전자공학과(공학사)
- 2000년 : 서울산업대학교 대학원 매체공학과(공학석사)
- 1994년 . 한국방송공사(KBS) 입사
- 2000 현재 . KBS 기술본부 방송망운용국 방송기기정비실
- 주관심분야 . 디지털TV 방송방식, 디지털 영상처리 NLE