碩士學位 請求論文

指導敎授 정 승 환

# 인터넷 방송에서 워터마킹을 이용한 디지털 컨텐츠 보호기법 분석

Digital Contents Protection By Watermarking
On The Internet Broadcasting

2002년 12월 일

한성대학교 컴퓨터 신기술 대학원
컴퓨터 신기술 학과 인터넷 방송 전공
백 진 호

碩士學位 請求論文

指導敎授 정 승 환

# 인터넷 방송에서 워터마킹을 이용한 디지털 컨텐츠 보호기법 분석

Digital Contents Protection By Watermarking
On The Internet Broadcasting

이 논문을 공학석사 학위논문으로 제출함

2002년 12월 일

한성대학교 컴퓨터 신기술 대학원
컴퓨터 신기술 학과 인터넷 방송 전공
백 진 호

백진호의 공학석사 학위논문을 인준함.

2002년 12월 일

심사 위원장 김 진 환 (인)

심사 위원 이 항 찬 (인)

심사 위원 정 승 환 (인)

# 요 약

디지털 컨텐츠 산업의 활성화에 따라 디지털 컨텐츠 저작권 보호 기술에 대한 관심이 고조되고 있다. 아날로그 시대에서는 컨텐츠의 불법 복사 및 사용에 대하여 관계 법령 및 제도적 조치로 어느 정도 이를 제한할 수 있었으나, 컨텐츠가 디지털화 됨으로써 더 이상 법적 구속력이나 제도적인 뒷받침만으로는 불법복제를 막을 수 없게 되었다. 따라서 점차 증가하고 있는 디지털 컨텐츠 산업을 육성하고 활성화하기 위해서 불법복제를 근본적으로 막을 수 있는 시스템에 대한 요구가 제기되었다. 이에 따라 디지털 컨텐츠를 보호하는 DRM(디지털 저작권 보호) 기술을 연구하였다. 또한 디지털 컨텐츠의 저작권을 디지털 워터마킹 방법에 대해 연구하고 Ingemar J. Cox가 제안한 방법을 이용하여 실험을 하여 워터마킹을 실제로 구현하였다. 실험 결과는 용량이 큰 이미지 파일일수록 검출이 어려웠으나, 원본의 이미지 보존율은 높게 나타났다.

# 목 차

# 그림 목차

# 표 목차

# 1장 서 론

## 1.1 연구배경

인터넷과 정보통신 기술의 비약적인 발전으로 인하여 어떠한 데이터라 하더라도 쉽게 구할 수 있게 되었다. 편집 및 수정이 용이한 디지털 정보는 복사 하여도 원본과 똑같게 복제되는 장점을 가지고 있다. 따라서 원하는 음악이나 동영상 등은 인터넷만 가능하다면 공유할 수 있고 전송 받을 수 있게 되었다.

그러나 이러한 무분별한 복제가 저작권 침해, 불법 복제 및 배포, 그리고 손쉽게 수정할 수 있기 때문에 많은 문제점을 내포하고 있다. 지난 2001년 7월 11일 샌프란시스코 연방 법원에서 mp3다운로드 서비스를 하는 냅스터에서 저작권이 있는 음악을 모두 차단하라는 명령을 내렸다. 그 후 1년이 지나 수원 지방법원 성남지원 민사 1부에서는 음반제작자들의 저작권이 있는 노래를 mp3형식으로 다운로드 받을 수 있게 해준 "소리바다" 운영자 양씨 형제에게 음반복제 금지 가처분 신청을 내려 2년여 운영해온 소리바다 서비스를 중단하게 되었다. 그 과정에서 음반 저작권자와 네티즌과의 찬반 논쟁이 끊임없이 이루어졌다.

또한 현재 미국에서는 저작권 관리 법안인 Consumer Broadband and Digital Television Promotion Act(CBDTPA)라는 것이 상원 의회에 계류 중이다. 콘텐츠를 다루는 모든 하드웨어와 소프트웨어에는 정부가 지정한 저작권 보호 시스템을 갖추는 것을 의무화해야 한다는 내용을 주요 내용으로 하고 있다. 월트 디즈니, 소니 등 엔터테인먼트 기업들은 이 법안을 환영하지만 인텔, Microsoft, 컴팩 등의 IT 기업들은 법률 실행의 실효성에 의문을 표명하고 있다. 온라인상의 저작권 보호는 오프라인처럼 보호 할 수가 없다는 것이다. 인터넷 이용자들은 그동안 무료 컨텐츠에 길들여져 있고 이른바 "정보공유"가 보편화 되어 있어서 그 법안에는 격렬히 반대하는 입장이다.

인터넷 비즈니스 업계가 대체적으로 성공하지 못한 데에는 사회 인식, 소비자의 의식, 비즈니스 모델, 기술도 따라야 하지만 디지털 컨텐츠의 저작권에 관한 법률도 포함된다.

저작권 관리 법안(CBDTPA)이 통과된다면 미국 정부가 지정한 저작권 보호 시스템을 갖추지 않은 가전 기기나 장치들은 미국 내에서 판매되지 못할 것이다. 국내에서 미국으로 제품을 수출한다 해도 시스템 장착을 위해 라이선스 비용이 추가되어 국내 업계는 큰 타격을 입게 될지도 모른다.

## 1.2 연구 목적 및 내용

우수한 디지털 미디어 컨텐츠의 소유자가 저작물을 판매 또는 홍보하기 전에 디지털 컨텐츠의 불법적 사용을 방지하는 안전한 전자 상거래 시스템이 있어야 한다. 그러한 모든 전자 상거래 시스템에 있어 중요한 구성 요소 중 하나가 디지털 저작권 관리 DRM(Digital Rights Management)이다.

또 하나는 텍스트, 이미지, 오디오, 비디오 등의 데이터에 소유주만 확인할 수 있는 마크(Mark)를 사람의 육안이나 귀로 구별할 수 없게 삽입하는 워터마크(Watermark) 기법이다. 만약 사용자가 멀티미디어 디지털 정보를 불법 복제하거나 정당한 대가나 허락 없이 사용 혹은 배포하였을 경우에 마크(Mark)를 추출하여 소유권 주장을 할 수가 있다.

정리하면 DRM은 디지털 컨텐츠의 생성에서 유통·관리까지 일괄적으로 지원하는 역할을 한다. 컨텐츠의 종류를 식별하고 위·변조를 막으면서 유통과정까지 추적할 수 있다. 사용료를 부과하고 결제대행 등을 할 수 있는 기능도 DRM이 제공한다. 위·변조를 막고 데이터 안에 기밀정보를 숨겼다가 분쟁이 났을 때 저작권자가 누구인지 확인해주는 역할을 워터마킹(Watermarking)이 하게 된다.

본 논문은 디지털 컨텐츠의 불법 복제를 디지털 저작권 관리(DRM)로 보호하고 불법으로 복제가 되었을 시에 소유권을 판별하는 Watermark 기법의 여러 가지 방법에 대해 알아보고, Cox가 제안한 Watermarking 기법을 실험해 보고 단점을 보완하는 방법에 대해 연구하는데 그 목적이 있다.

## 1.3 국내 웹캐스팅 업체 현황

웹캐스팅 업체는 1997년 7월 M2station을 최초로 국내에서 접근되기 시작했고 매년 급성장세를 거듭하고 있다. 실질적인 업계 진입시기인 1998년을 기점으로 1999년이 전년대비 250% 성장, 2000년이 전년대비 450%(2000년 연말 900개 기준으로 한 추정치) 성장을 보이고 있다. 특히 인터넷 비즈니스와 벤처산업에 대한 사회적 수요가 높았던 1999년 하반기에서 2000년 상반기까지 급증세를 보였다[12]. 2001년에 접어들어서는 경기침체와 시장상황의 열악함으로 인해 웹캐스팅 사업체의 증가율은 둔화되고 있으며, 고착화 현상도 보이고 있다. 특히 2001년 상반기를 기점으로 다수 웹캐스팅 업체에서 사업 분야 축소나 구조조정, 사업포기 등을 단행한바 있다[14].

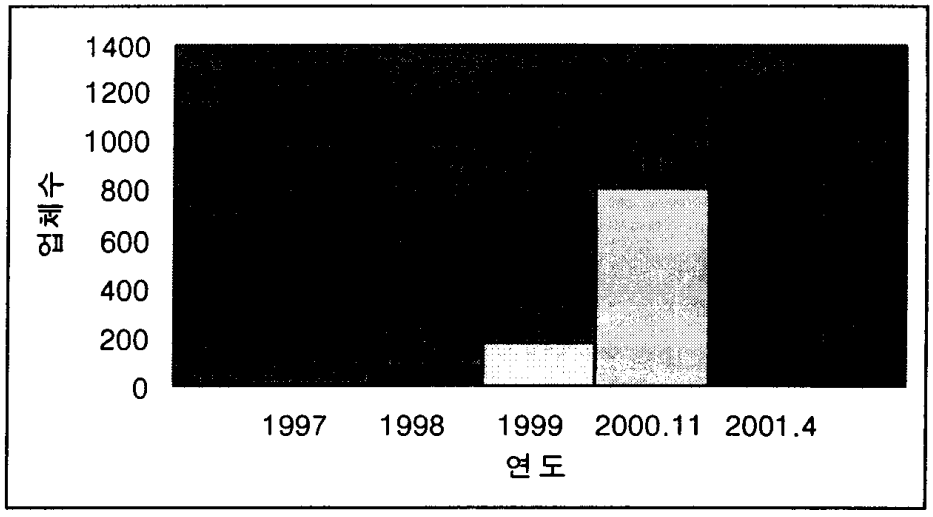



그림 1.1 국내 웹캐스팅 업체 현황

## 1.4 인터넷 방송업체의 매출현황

매출액 면에서도 인터넷 방송시장은 1999년 48억원에 불과하였으나 2000년 상반기에는 128억, 2000년 하반기에는 657억원의 규모를 나타내며 상반기 대비 410% 가량 큰 성장을 보였다.

표 1.1 국내 인터넷 방송국 매출 현황

(단위 : 백만원 (백분율(%))

| 구분 | 회원 가입비 | 이용료 | 광고수입 | 수주 개발수입 | 기타수입 | 전체 |
|---|---|---|---|---|---|---|
| 1999년 | 99<br>(2.05) | 202<br>(4.18) | 657<br>(13.59) | 2,791<br>(57.74) | 1,085<br>(22.45) | 4,834 |
| 2000년 상반기 | 687<br>(2.05) | 3,657<br>(4.18) | 2,513<br>(13.59) | -<br>(0.00) | 6,024<br>(46.77) | 12,881 |
| 2000년 하반기 | 5,282<br>(8.03) | 9,098<br>(13.83) | 5,844<br>(8.88) | 26,794<br>(40.73) | 18,764<br>(28.52) | 65,782 |

## 1.5 디지털 콘텐츠 사업자의 컨텐츠 유료화

인터넷이 보편화 되면서 수많은 닷컴 기업들은 유용한 정보와 컨텐츠 그리고 가입 이벤트 경품으로 무료 회원을 유치하여 회원수에 비례하는 광고 수입을 얻었다. 광고 수익이 수익사업에 가장 큰 부분을 차지하였다.

1999년 매출 현황을 보면 광고 수입이 이용료 수입보다 더 높은 것으로 조사되었지만 2000년 하반기에는 광고수입보다 컨텐츠 이용료의 비율이 높은 것으로 나타났다. 2000년 하반기부터는 온라인 광고의 실효성이 줄어들면서 업체 수익구조의 컨텐츠 이용요금이 비중이 높아졌다. 그만큼 디지털 컨텐츠 수익사업에 있어 컨텐츠 이용요금이 광고수입보다 더 중요하게 부각 되었고 컨텐츠가 복제 혹은 배포가 되지 않도록 하는 보안이 더 중요한 부분으로 작용하게 되었다[21].

2001년 10월 sbs社가 방송 프로그램 다시보기 서비스를 유료화로 전환하여 대표적인 성공한 사례로 평가되고 있다. 지난달에는 KBS에서 디지털 컨텐츠 유통 사이트인 콘피아(www.conpia.com)를 개설하여 고화질의 컨텐츠를 국영방송인 것을 반영해 KBS홈페이지(www.kbs.co.kr)가 아닌 다른 곳에서 우회적으로 판매를 개시하였다. 올해 초부터 유료화를 검토하던 MBC도 올해 안에 유료화로 전환할 계획에 있다고 한다[2].

이렇게 컨텐츠를 판매 하게 되면 인터넷은 무료라고 항상 여겨왔던 유저들은 어떻게든 무료로 동영상을 받고 싶어 할 것이다. 만약 인기 있는 프로그램이라면 한사람이라도 다운을 받아서 인터넷에 게시하게 된다면 수십 개의 또 다른 곳에 올려져 급속도로 널리 퍼지게 된다. 저작권이 명시되어있는 비디오테이프 같은 오프라인상의 매체가 아닌 디지털 매체이기 때문에 급속하게 구축된 인터넷 인프라에 의해 전파되는 것이다.

예를 들면 미국에서 개봉한 스타워즈 에피소드2는 개봉하기도 전에 인터넷에서 쉽게 구할 수 있을 정도로 배포가 되어 영화가 크게 흥행하지 못하고 큰 손실을 가져다주었다.

유료화 된 컨텐츠가 무단 불법 복제 및 유통이 되고 위변조가 이루어지게 된다면 수익률과 창작열이 저하가 되고 이미 유료로 컨텐츠를 이용한 고객의 충성도가 하락하게 되어 회원 탈퇴 등이 이루어지게 될 것이다. 웹 비즈니스 시장에서 유료 컨텐츠 이용에 따른 수익구조가 중요해진 만큼 컨텐츠 무단 복제는 콘텐츠 기업들에게 큰 손실을 주게 된다.

# 2 장 관련 연구

## 2.1 인터넷 스트리밍 파일의 개념

### 2.1.1 ASF(Active Streaming Format) 파일의 개요

개발자들이 실시간 스트리밍 미디어 솔루션을 개발하려고 할 때 기존의 멀티미디어 파일 포맷(WAV와 AVI)이 적합하지 않다는 것을 파악하였다. WAV와 AVI는 개인PC에서 동작하기에는 무리가 없지만 인터넷 방송용으로는 여러 가지 문제점이 있기 때문에 스트리밍용 파일을 연구하게 되었다.

멀티미디어를 스트리밍 하려면 여러 개의 스트림을 공통 시간대로 동기화해야 하는데 WAV와 AVI 포맷 파일에는 동기화 할 수 있는 데이터가 없어 다른 스크립트로 동기화를 이루어야 하는 단점이 있다.

또한 WAV와 AVI포맷파일은 RIFF(Resource Interchange File Format)규정을 준수하는데 RIFF 파일은 청크(chunk) 라는 데이터 단위로 구성된다. 각 청크의 헤더에는 청크의 크기를 바이트로 규정한 32비트의 길이 필드가 들어 있는데 32비트 필드를 사용하면 청크의 크기가 4기가바이트로 제한되는 단점이 있었다. 반면 ASF에서는 청크를 객체로 대체해 ASF객체는 64비트 길이 필드를 사용하여 객체의 크기를 지정함으로 길이 필드

가 32비트에서 64비트로 늘어났기 때문에 ASF객체의 크기가 RIFF 청크보다 더욱 커질 수 있는 것이다. 그래서 ASF 객체에는 잠재적으로 수 시간에 이르는 비디오와 오디오를 담을 수 있다.

Microsoft사가 1996년에 멀티미디어 스트리밍용으로 특별히 고안된 첫 번째 파일 포맷인 ASF는 같은 시간으로 동기화 된 오디오, 비디오, 텍스트(캡션), 이벤트의 압축된 디지털 버전을 포함하고 있다. ASF는 멀티미디어 데이터를 다양한 대역폭으로 네트워크에 효율적으로 전송하고, 적용하며 네트워크 조건을 변경하는 데 적합한 뛰어난 포맷이다.

### 2.1.2 ASX

Windows Media Technologies의 초창기에는 브라우저가 스트리밍 미디어에 사용되는 프로토콜을 사용하지 않았기 때문에 웹 페이지에서 Windows Media 서버로 직접 링크시키기가 힘들었다. 이런 문제를 해결하기 위해서 Windows Media 서버에 있는 제목에 대한 참조가 들어 있는 ASF Stream Redirector 파일을 만들게 되었다. 실제 동영상 asf 혹은 wmv 파일이 있는 위치를 redirect 하기 때문에 HTML 로 보이는 화면에서는 바로 동영상을 다운로드 할 수 가 없다. asx 파일을 만들어 Redirect 하는 것은 컨텐츠를 보호하는 가장 기초적인 방법이다. 그러나 이것은 asx 파일 형식만 조금만 알고 있다면 컨텐츠를 받을 수 있다.

## 2.2 DRM(Digital Rights Management)

### 2.2.1 DRM 이란

DRM은 Digital Rights Management로 컨텐츠 공급자에게 디지털 미디어 컨텐츠를 안전하게 판매 혹은 게시 할 수 있는 유연한 플랫폼을 제공하는 디지털 권한 관리 시스템이다. 즉 DRM은 디지털 컨텐츠에 대한 적법한 사용을 인증해주고, 합법적인 유통을 보장해주는 기술과 서비스를 총칭하는 말이다[2].

컨텐츠 소유자는 배포가 제한된 형식으로 인터넷을 통해 음악, 비디오 및 기타 미디어를 무단복제에 대한 걱정 없이 자유롭게 전달할 수 있게 하는 기술이다. 서론에서도 언급했듯이 음반 산업이 MP3 공유 프로그램으로 인해 많은 위협을 받게 되었다. 아무런 생각 없이 저작권이 있는 음악 파일을 다운로드 받는 것이 저작권 침해 행위가 되는 것이었다. 이러한 문제점을 해결하기 위해 여러 음반 산업 단체와 기술 관련 회사들이 함께 모여 온라인 배포로 발생할 수 있는 위험으로부터 예술가와 음반 회사들을 보호하는 디지털 권한 관리(Digital Rights Management)를 개발하였고, 그 노력으로 SDMI (Secure Digital Music Initiative)를 만들게 되었다. SDMI의 표준을 구현하면 음반 회사들은 MP3를 불법 복제로부터 보호하고 음악가에서 온라인 배포자 까지 이 작업에 관련된 모든 사람들을 보상해줄 수 있게 되었다.

디지털 컨텐츠의 보호는 MP3만 해당되는 것은 아니다. 음악 뿐만 아니라 중요한 텍스트 문서 파일부터 막대한 자금을 들여 제작한 영화까지 다양한 컨텐츠들이 보호 대상이 된다. 대형 블록버스터인 스타워즈가 막대한 자금으로 영화를 만들었다 해도 디지털화된 파일은 전 세계 곳곳으로 퍼져 극장 이용료를 부담하지 않고 볼 수 있는 것이다.

DRM은 컨텐츠를 이용하는 자가 적법한 사용자임을 인증하여 콘텐츠 판매에 기여하는 기본 기능 이외에도 여러 가지 부가적인 기능을 제공하고 있다. 다양한 사용자 권한 설정을 해줄 수 있다는 것이다. 즉 몇 번이나 다시 볼 수 있는지에 대한 실행 가능 횟수, 실행 가능 시간, 출력이 가능한지에 대한 허용 여부, 다른 PC에서 사용한지에 관한 여부, 개인 단말기로의 전송(다운로드) 허용 여부 등을 설정할 수가 있어 다양한 모델에 적용이 가능하다. 한번만 보여주는 컨텐츠는 실시간 스트리밍으로 전송하여 주고, 교육 컨텐츠 등 여러 번 반복해서 이용해야 하는 것은 다운로드를 할 수 있도록 설정할 수가 있다.

### 2.2.2 DRM의 기능

DRM이 컨텐츠를 단순히 보호하는 기능도 하지만 DRM 시스템의 진정한 목적은 컨텐츠 제공업자(CP)와 콘텐츠 사용자 간의 1:1 관계뿐만 아니라 유통의 기능까지 가능하게 하는 것이다.

단순히 'CP-사용자' 만으로는 트랜잭션(Transaction)을 키울 수 없다. 'CP-CP', '사용자-사용자' 등의 경로를 통해서도 활발한 거래가 이루어 져야 수익성을 높일 수 있다.

냅스터, 소리바다, 당나귀(eDonkey) 등의 프로그램이 P2P(Peer to peer)를 이용하여 사용자와 사용자간에 자료를 주고받을 수 있게 하였기 때문에 엄청난 양의 디지털 컨텐츠를 주고받을 수 있는 것이다. 사용자-사용자의 경로를 이용한다면 CP-사용자의 경로보다 빠른 속도로 전파가 되어 더 많은 사람들이 DRM 시스템을 거친 컨텐츠를 얻게 된다.

이렇게 얻어진 컨텐츠는 이용자들이 보고 싶어 하게 되고 보기 위해서는 DRM 시스템을 거쳐 인증이나 요금 결제를 하게 되는 것이다. 마치 게임을 발표하기 전에 정품과 달리 기능이 많이 제약된 데모 버전을 무료로 배포하고 정품 구입을 유도하거나 사용기간이 정해져 있는 프로그램을 무료로 다운로드 받게 하여 등록 기간이 지나면 사용할 수 없게 하는 셰어웨어(Shareware)와 비슷한 논리이다. 이러한 DRM의 여러 기능들을 현재 가장 널리 쓰이고 있는 Microsoft社의 DRM 기술인 Windows Media Rights Manager를 기준으로 살펴보면 다음과 같다.

### 2.2.3 디지털 미디어의 안전한 배포

컨텐츠 소유자의 권리를 보호함과 동시에, 소비자가 쉽고 합법적으로 디지털 컨텐츠를 얻을 수 있도록 해주는 보안 기술이다. CP와 사용자 간에 소극적인 유통에 적합하다.

### 1) 영구 보호

인터넷을 통하여 널리 배포 된 디지털 컨텐츠라 할지라도 "잠금"장치가 되어있어 라이선스를 얻지 못한 이용자는 컨텐츠를 관람 할 수 없다. 각 컴퓨터마다 고유하게 할당된 라이선스는 이미 라이선스를 받은 사람과 복제하여 받은 사람과 구별되기 때문에 실제 사용자인지 아닌지를 분별할 수 있다.

### 2) 강력한 암호화

Rights Manager에는 배포된 디지털 미디어 파일이 저작권 침해 또는 기타 불법적 사용에 노출되는 것을 방지하는 입증된 암호화 스키마가 포함되어 있기 때문에 쉽게 수정하거나 변조할 수 없다.

### 3) 개별화

플레이어를 호스트 컴퓨터에 연결하여 각각의 플레이어를 고유화한다. 이렇게 하면 손상된 플레이어가 인터넷에 널리 배포되는 것을 방지할 수 있습니다. 개별화를 통해 라이센싱(또는 사용권 허가) 프로세스시에 손상된 플레이어를 식별하여 사용할 수 없도록 할 수 있다.

### 4) 보안 경로

디지털 컨텐츠가 서버에서 사용자 PC까지 도달되어 PC에서 플레이 될 때까지의 경로가 노출 되지 않게 설계 하여서 이용자

가 중간에 스트리밍을 캡쳐하여 저장 하지 못하도록 하였다.

#### 5) 향상된 사용 해제 기능

수정 및 변조된 디지털 컨텐츠를 플레이 하려고 할 때 정상적으로 보이지 않도록 하는 기능이다. 디지털 컨텐츠를 관람 이외의 어떠한 목적으로 변조하게 되면 컨텐츠는 그 기능을 잃어버리게 된다.

#### 6) 안전한 앤드-투-앤드 스트리밍 및 다운로드

디지털 미디어 파일은 보안 암호화 프로토콜을 통해 다운로드 시에 보호되며 소비자 PC 상에서도 보호됩니다.

### 2.2.4 유연한 비즈니스 모델

Rights Manager는 미디어의 안전한 배포에서 보다 더 유연하게 배포 되는 방법이다.

#### 1) 개별 배포되는 라이선스 및 미디어

컨텐츠 제공업체가 제공하는 미디어 파일과는 별개로 라이선스가 발급되어 콘텐츠가 여러 곳에 쉽게 배포 되게 하여 컨텐츠를 보려 하는 이용자에게 라이선스 권유를 하는 방법이다. 소비

자의 컴퓨터에 라이선스가 있는지를 확인한 후 유효한 라이선스를 가지지 않은 이용자에게는 라이선스를 거치도록 하게 된다.

### 2) 사용권 허가 조건 변경의 용이성

라이선스와 디지털 미디어 파일은 별도로 저장되므로 디지털 미디어 파일을 다시 배포하거나 패키지 처리하지 않고도 서버 상에서 라이선스 조건을 변경할 수 있습니다. 만약 라이선스와 미디어 파일이 함께 포함되어 있다면 라이선스를 변경하기 위해서는 컨텐츠를 함께 관리해야 하는데 별도로 저장된다면 서버에서 간단히 변경함으로써 이미 배포된 라이선스까지 변경할 수 있다.

### 3) 혁신적인 임대 또는 가입 모델

컨텐츠 공급자는 혁신적인 비즈니스 모델을 만들기 위해 라이선스의 시작 시간, 중지 시간 및 기간을 제어할 수 있습니다. 이와 같이 다양한 권한을 사용하면 컨텐츠 공급자는 고유의 비즈니스 규칙을 최적화할 수 있습니다.

### 4) 제한된 재생 미리보기

새 라이선스 구조에 포함된 작업(재생) 옵션을 사용하면 컨텐츠 공급자는 디지털 미디어 파일을 볼 수 있는 임대(rental) 또는 미리보기 라이선스를 만들어 배포할 수 있다.

### 2.2.5 Microsoft의 DRM 최근 기술

Microsoft Windows Media SDK의 주요 구성 요소 중 하나인 Microsoft Windows Media Rights Manager 7.1 SDK(Software Development Kit)를 사용하면 개발자가 Windows Media 기반의 파일을 보호하고 라이선스를 발급하는 서버측 응용 프로그램을 만들 수 있다. 보안성과 유연성을 증가시키고 컨텐츠 공급자의 요구를 충족시킬 수 있는 보다 견고한 솔루션을 제공하기 위해 DRM (디지털 저작권 관리)을 지속적으로 개발되고 있다.

#### 1) 비즈니스 Rules

• 처음 사용 이후 만료

라이선스를 처음 사용한 이후부터 라이선스의 유효 시간(시간 단위) 길이를 지정한다. 예를 들어, 소비자가 Windows Media 파일의 재생을 시작한 후 24시간 내에 만료하도록 라이선스를 설정할 수 있습니다. 이용자가 결제 한 후 지정된 시간 내에는 무제한으로 원하는 시간에 볼 수 있게 하는 방식이다. 현재 유료 컨텐츠 사이트에는 대부분이 이 Rule을 사용한다.

• 처음 저장 시 만료

이 권한은 소비자의 컴퓨터에 라이선스가 처음으로 저장된 후부터 라이선스의 유효 시간(시간 단위) 길이를 지정한다. 라이선스가 완료되어 이용자의 PC에 다운로드가 완료된 시점으로부터 시간단위로 만기를 지정할 수 있다.

• 보호된 스트림의 저장 허용

패키지화된 Windows Media 파일이 스트리밍되는 경우 이 권한은 소비자가 스트림을 파일 형태로 저장할 수 있도록 한다. 저장된 파일은 패키지화된 상태로 유지되며 여전히 라이선스가 필요합니다. 저장은 허용하되 라이선스가 유효하도록 설정 한다.

### 2) 컨텐츠 헤더의 동적 수정

수정된 패키지 파일을 디스크에 저장하지 않고서도 컨텐츠 헤더를 동적으로 수정할 수 있다. 결과적으로 소비자가 패키지화된 파일을 다운로드하기 전에 즉석에서 파일 안에 정보(고객 특성 등)를 포함시킬 수 있다. 따라서 비즈니스 모델에 따라 패키지 프로세스가 진행되는 동안 서로 다른 시간에 여러 관계자들이 컨텐츠 헤더를 수정할 수 있다.

예를 들어, 컨텐츠 소유자가 여러 공급업체와 계약을 했을 경우 소유자는 동적 컨텐츠 헤더 수정의 기능을 사용하여 파일이 처음 패키지화될 당시 알려지지 않았던 공급업체의 확인 정보를 포함시키게 된다. 컨텐츠소비자가 다운로드 하기 바로 전에 컨텐츠 소유자는 공급업체의 ID를 고객 특성으로 컨텐츠 헤더에 추가한다. 그런 다음 소비자가 패키지화된 파일에 대한 라이선스를 얻을 경우 라이선스 발급자는 어떠한 공급업체가 판매에 대한 책임이 있는지를 컨텐츠 헤더에서 확인할 수 있습니다. 소비자가 패키지화된 파일을 친구와 공유할 경우 본래의 공급업체는 친구가 구매한 모든 추가적 라이선스에 대한 판매를 신뢰할 수 있다.

### 3) 플레이어 응용 프로그램 제외

플레이어 응용 프로그램 제외 기능은 라이선스 발급 자가 특정 플레이어 응용 프로그램이 패키지화된 특정 파일을 재생할 수 없도록 제한하는 기능이다.

이 기능은 라이선스를 통해 클라이언트에 적용된다. 패키지화된 파일에 대한 라이선스를 생성할 경우, 라이선스 발급 자는 제외시킬 플레이어 응용 프로그램의 ID를 지정합니다. 따라서 소비자는 제외된 플레이어 응용 프로그램 상에서 패키지화된 파일을 재생할 수 없다. 이 기능의 이점은 제외된 플레이어 응용 프로그램에는 어떠한 영향도 미치지 않는다는 점이다. 단지 패키지화된 파일을 사용할 수 없을 뿐이다.

### 4) 보호 콘텐츠 매니저 제외

패키지 파일을 사용하는 플레이어는 콘텐츠를 암호화 및 해독하며 라이선스 권한을 시행하는 보호된 컨텐츠 매니저를 포함한다. 보호된 콘텐츠 매니저 제외 기능은 손상된 보호 콘텐츠 매니저에 기초하여 플레이어 응용 프로그램을 식별할 수 있도록 하는 기능이다.

이 기능은 라이선스 서버를 통해 적용된다. Microsoft는 라이선스 발급 자가 반드시 획득하여 정기적으로 업데이트 해야 하는 보호 콘텐츠 매니저 제외 목록을 게시합니다. 그러면 제외된 보호 콘텐츠 매니저를 기초로 하는 플레이어로부터 라이선스 발급 자가 라

이선스 요청을 받을 경우 라이선스 발급 자는 라이선스 발급을 거절할 수 있다. 대신에 새 플레이어 또는 업그레이드를 다운로드할 수 있는 링크를 표시할 수 있다.

### 5) SDK 보안 수준

패키지화된 파일을 사용하기 위해 플레이어 응용 프로그램의 기초가 되어야 하는 Windows Media Format SDK의 최소 보안 수준을 지정할 수 있는 새로운 권한이 추가된다.

패키지 파일을 지원하는 모든 플레이어 응용 프로그램에는 Windows Media Format SDK를 기초로 하는 구성 요소가 있다. Windows Media Format 7.1 SDK에는 코덱의 서명 확인을 포함하여 많은 개선이 있었다. 또한 Windows Media Format 7.1 SDK 이상을 기초로 하는 플레이어만이 이 문서에서 설명한 새로운 기능을 해석할 수 있다. 그러므로 최신 보안 기능을 사용하려면 이 새 권한을 사용하여 Windows Media Format 7.1 SDK 이상에 해당하는 최소 SDK 보안 수준을 보유하도록 플레이어에 요청할 수 있다.

## 2.2.6 Windows Media Rights Manager 의 구조

마이크로소프트사의 Windows Media Rights Manager 구조를 살펴보면 그림 2.1과 같이 7개 단계를 거쳐 이루어진다. 그중 기본적인 5개 단계를 살펴보면 다음과 같다[22].

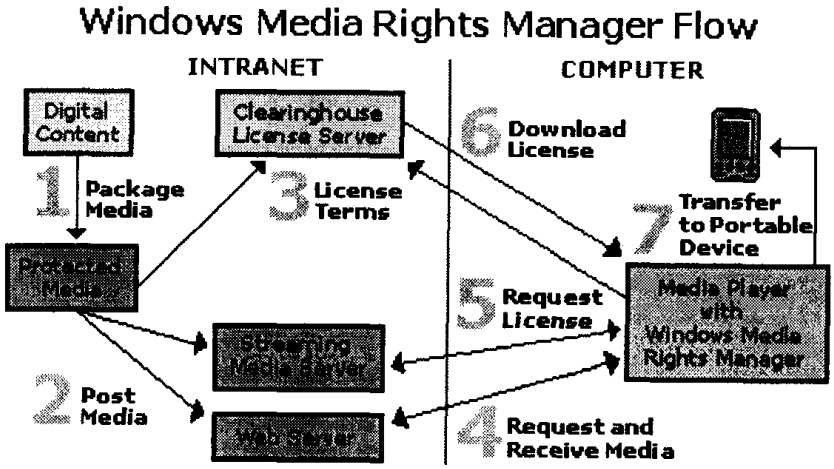



그림 2.1 Windows Media Rights Manager Flow

### 1) 패키지화

Windows Media Rights Manager는 디지털 미디어 파일을 패키지화한다. 패키지 된 미디어 파일은 key에 따라 잠겨지고 부호화 된다. 그 키는 부호화된 라이선스에 미디어 파일과는 별개로 저장된다. 어디에 라이선스가 있는지 URL등의 다른 정보들도 미디어 파일에 추가된다. 이 패키지 된 디지털 미디어 파일은 Windows Media Audio format (.wma 확장자를 가진 파일) 혹은 Windows Media Video format (.wmv 확장자를 가진 파일)로 저장된다.

### 2) 분배

패키지화된 파일은 다운로드 가능하도록 웹 사이트에 위치될 수 있다. 미디어 서버에서 스트리밍을 위한 미디어, CD-ROM, 고객

에 전달되는 e-mail에 분배가 된다. Windows Media Rights 매니저는 이용자의 친구들에게 복사 금지된 디지털 미디어 파일을 보내는 것을 허락 할 수 있다.

### 3) 라이선스 서버 수립

컨텐츠 제공자는 Windows Media Rights Manager 라이선스 서비스 그리고 라이선스의 특별한 저작권과 rule을 저장하는 '라이선스 clearing house'를 선택한다. Clearing house의 역할은 라이선스에 대한 고객의 요구에 인증해 주는 것이다. 디지털 미디어 파일과 라이선스는 분류되어 따로 저장되어 완전한 시스템을 관리하기 쉽게 해준다.

### 4) 라이선스 획득

패키지 된 디지털 미디어 파일을 재생시키기 위해서 고객은 파일의 잠금장치를 열수 있는 라이선스 키를 최초로 얻어야만 한다. 그 과정은 보호된 컨텐츠를 획득하려고 시도 혹은 최초에 파일을 플레이 하면서 자동으로 시작된다. Windows Media Rights Manager는 clearing house에서 라이선스를 돌려받거나 요구된 지불을 요구하는 정보가 있는 등록 페이지를 보낸다.

### 5) 미디어 파일의 재생

디지털 미디어 파일을 재생하기 위해서는 Windows Media

Rights Manager를 지원하는 미디어 플레이어가 필요하다. 이용자는 라이선스가 포함된 저작권이나 rule(재생 수, 제한 시간, 등등)에 따라서 디지털 미디어를 플레이할 수 있다.

라이선스는 시작 시간과 날짜, 기간, 실행수를 각각 다르게 포함할 수 있다. 예를 들어 PDA, 휴대폰등 포터블 장치에 복사한다든지, 다른 컴퓨터에 플레이 할 수 있는지를 허락할 수 있다. 그러나 라이선스는 전송 할 수 없다. 만약에 이용자가 패키지 된 디지털 미디어 파일을 친구에게 전송한다면 그 친구는 파일을 재생하기 위해선 자신의 라이선스를 획득해야만 한다. PC와 PC의 라이선스는 파일을 위한 라이선스 키를 받은 컴퓨터에서만 재생될 수 있다.

### 2.2.7 라이선스와 key

컨텐츠 소유자는 패키지 파일을 만들기 위해 Key를 포함시켜 컨텐츠를 잠근다. 고객이 파일을 플레이하기 전에 라이선스 clearing house는 고객의 PC에 다운로드할 수 있는 라이선스와 패키지 파일의 잠금장치를 풀 수 있는 라이선스를 만든다. 아래의 그림은 Windows Media rights Manager가 어떻게 키가 만들어지는지를 보여준다[22].

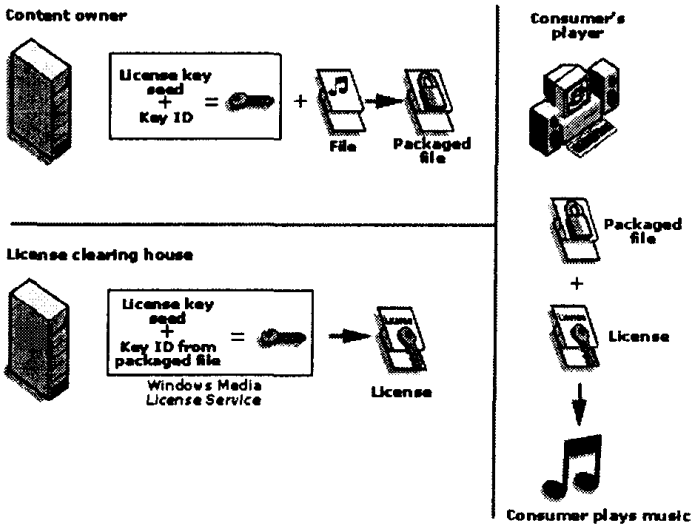



그림 2.2 라이선스와 키

키를 생성하기 위해서 라이선스 키 생성자와 키 ID가 필요하다 : 라이선스 키 생성자는 컨텐츠 저작권자와 라이선스 clearing house만을 위해 알려진 값이다.

key ID는 윈도우즈 미디어 파일을 위한 컨텐츠 저작권자에 의해서만 생성된다. 그 값은 패키지 된 파일 안에 포함된다.

라이선스 clearing house가 패키지 된 파일을 위한 라이선스의 발행이 필요할 때, 키는 패키지 된 파일로부터 키 ID 회수하면 재생산된다. Windows Media License Service는 라이선스 키 생성자를 사용한다. 그 키는 고객의 컴퓨터에 보내진 라이선스 안에 포함된다. 라이선스에 포함된 키의 사용은 고객의 컴퓨터의 플레이어가 보호된 파일을 오픈하고 재생할 수 있게 한다.

### 2.2.8 라이선스의 동작원리

각각의 라이선스는 미디어 파일을 잠글 수 있는 키를 내포하고 있다. 그 라이선스는 저작권, 디지털 미디어 파일의 사용을 제어할 수 있는 rule도 내장하고 있다. Windows Media Rights Manager 라이선스는 각기 다른 비즈니스 rule의 넓은 범위를 다음과 같이 지원할 수 있다.

- 얼마나 많이 파일을 재생할 수 있는가에 대한 rule.
- 어떤 장치에 전송이 되어 재생될 수 있는지에 대한 rule. 예를 들면 portable 장치(PDA, 휴대폰) 혹은 Secure Digital Music Initiative (SDMI)가 장착된 플레이어 등에 전송할 수 있는지에 대한 rule.
- 이용자가 파일을 재생할 때 만기 날짜가 언제인지 알려 줄 수 있다.
- 파일이 UD 레코더로 저장될 수 있는지에 대한 rule.
- 이용자가 라이선스를 재 저장하거나 백업할 수 있는지에 대한 rule.

비즈니스 모델에 따라 라이선스는 다른 시간에 그리고 다른 경로로 배달될 수 있다. 이용자가 다운로드하고, 패키지 된 파일을 처음으로 재생하려고 할 때 라이선스를 받는 경우 혹은 그 이전에 받을 수 있다.

## 2.3 워터마킹(Watermarking)

### 2.3.1 워터마크의 유래

워터마크(Watermark)는 고대 이집트에서 파피루스(종이)를 만드는 과정에서 섬유질을 물에 풀었다가 물을 압착하기 위해 틀을 사용하는 과정에서 나온 마크를 뜻한다. 중세에는 작전명령서 등 기밀문서의 안전한 배송을 위해, 혹은 연애편지와 같은 개인적인 메시지 전달을 위해 사용되기도 하였고, 제지업자들은 자신들의 고유 상품임을 증명하기 위해 종이에 마크를 삽입하기도 했었다.

지폐를 제조하는 과정에서 종이가 젖어 있을 때 인쇄를 하고 말린 후 양면에 인쇄를 하면 빛을 통해서만 확인할 수 있는 그림이 들어가게 된다. 현대에 와서 이 기법을 써서 지폐를 제조하였고 이것은 위조지폐를 확인 하는 방법으로 쓰인다. 미 항공 우주국(NASA)을 비롯해 미 연방 수사국(FBI) 등에서 보안 기술 중의 하나로 활용 되고 있다.

오늘날 디지털 멀티미디어의 발달에 따라 디지털 워터마크라는 개념이 등장하게 되었고, 기존의 오프라인 상에서의 워터마크의 성격과는 다른 온라인에 적용되기 시작하면서 그 개념이 확산되고 있다. 단순 저작자 표시 이외에 디지털 컨텐츠에 관한 정보(입력시간, 입력자, 입력 장소 등)를 다양하게 삽입할 수도 있다.

### 2.3.2 디지털 워터마킹의 정의와 일반적 특성

디지털 워터마킹이란 이미지, 영상, 음악 등의 멀티미디어 디지털 저작물의 저작권을 보호하거나 위·변조를 감별하고 추적하기 위해서 특수한 형태의 워터마크를 삽입하고(Embedding), 검출(Detecting)하는 기술적 방법을 뜻한다. 저작물 데이터의 전부를 바꾸는 암호화와는 달리 워터마크 삽입 후에도 원본 신호를 유지하는 것이 특징이다. 암호화의 기본 특성은 권한이 없는 사람들의 데이터에 대한 접근 권한을 제한함으로써 복제 방지나 기타 보안을 유지하는 것이다. 이는 저작물에 대해서 지불/결제 과정을 거치지 않은 일반 사용자들의 접근 자체를 봉쇄하는 것이며, 개념적으로는 암호화가 풀린 이후의 상황에서는 컨텐츠 보호가 어려운 상황이 초래될 수 있다.

이와는 달리 워터마킹 기술은 데이터에 대해 접근 제한을 두지 않으며, 워터마크는 항상 저작물 자체에 존재하므로 언제든지 검출할 수 있다. 또한 워터마킹은 사전적 의미의 보호시스템인 DRM과는 달리 사후적 의미의 저작권 보호 관리 툴이라고 할 수 있다. 즉 특정 이미지의 저작권자가 이미지를 생성해 온라인으로 배포함에 앞서 워터마크를 삽입한 후에 불법적인 사용 사실을 인지하게 되면 그 이미지를 회수해 추출하게 되는데 이때 검출된 워터마크를 증빙자료로 불법 사용자에게 법적인 압력을 행사할 수 있게 된다.

이런 과정을 가능케 하는 것은 바로 워터마킹 기술의 '비가시성'이다. 워터마킹 기술은 워터마크를 삽입한 후에도 화질이나, 음질, 이미지에 변화가 없이 인간의 시각이나 청각으로 감지하지 못하도

록 아주 미세하게 삽입해 워터마크 삽입여부를 알 수 없게 하는 것을 기본적이고 중요한 특성으로 한다. 이러한 워터마크를 'Imperceptible 워터마크'라고 한다. 만일 저작권 정보를 담고 있는 워터마크에 쉽게 접근할 수 있다면 마크를 변형해 없애는 공격이 가능하기 때문에 저작권 보호라는 본래의 목적을 달성하기 어려울 것이다.

물론 비인지성과는 달리 뚜렷하게 워터마크를 표시해 디지털 저작물의 복제 및 불법 사용을 억제하는 효과를 가질 수도 있는데 이를 'Perceptible 워터마킹'이라고 한다. 방송사나 음반사들이 주로 사용하는 방식으로 원리 사후적 툴인 워터마킹을 사전에 심리적으로나마 불법 행위에 대한 부담감을 지우려는 의도로 사용되기도 한다.

### 2.3.3 디지털 워터마킹의 방법 및 용도

워터마킹 방법은 다양한 목적으로 사용 될 수 있다. 워터마킹을 사용하는 여러 가지 용도는 다음과 같다.

#### 1) Ownership assertion

이것은 디지털 미디어 컨텐츠의 소유관계를 주장하는 방법으로 워터마크를 사용하는 것이다. 컨텐츠에 대한 소유를 주장하기 위해서, 먼저 컨텐츠를 만드는 작가는 비밀 키를 사용해서

워터마크를 생성한 뒤 그것을 원본 컨텐츠에 삽입을 한다. 그런 뒤 작가는 워터마크가 삽입된 이미지를 공개한다. 나중에 다른 사람이 이 공개된 컨텐츠의 소유를 주장하면 원래 컨텐츠를 생성한 작가는 워터마크가 없는 원본 컨텐츠를 생성해서 소유를 주장하는 다른 사람의 이미지에 자신이 삽입한 워터마크가 있음을 보여주면 되는 것이다. 이때 작가의 원본 컨텐츠는 소유를 주장하는 다른 사람에게는 알려지지 않았으므로 다른 사람은 작가처럼 자신의 소유를 주장할 수 없게 된다. 하지만 이런 방법이 동작하기 위해서는 이미지에 대한 압축, 확대, 축소 등과 같은 연산을 수행해도 워터마크가 없어지지 않고 남아 있어야 한다.

### 2) Fingerprinting

이 방법은 디지털 미디어의 무단 복제와 무단 배포를 막기 위한 방법이다. 먼저 컨텐츠의 저자는 각각의 데이터 카피에 대해서 유일한 워터마크를 부여해서 그 데이터 카피에 삽입을 한다. 만일 무단으로 복사된 컨텐츠가 발견되면 카피 내에 숨겨져 있던 워터마크는 변하지 않았으므로 카피의 원본이 어떤 것인지를 알아내어 불법 복사를 한 사람을 찾아 낼 수 있게 된다. 이 방법이 동작하려면 워터마크를 삭제하려 하거나 워터마크가 동작하지 못하도록 하려는 여러 가지 시도에 대해서 안전해야만 한다.

### 3) Authentication and integrity verification

이것은 멀티미디어 컨텐츠가 법적인 용도, 의학적인 용도, 뉴스 또는 상업적인 용도로 사용되는 경우에 컨텐츠를 만든 창작자가 누구인지 확인함과 동시에 그 미디어가 훼손되거나 수정되지 않았다는 무결성(integrity)을 확인하는 것이다. 일반적인 인증(authentication)은 암호학적인 방법을 사용해서 해결할 수 있다. 하지만 워터마킹 방법을 사용하면 컨텐츠에 대한 인증을 수행하는 부분이 컨텐츠에 포함이 되어 데이터를 처리하는 문제를 간단히 할 수 있게 된다. 이 방법이 동작하려면 이미지의 변경에 대해 확인 가능한 장치가 있어야 한다.

### 4) Content labeling

이것은 워터마크를 사용해서 컨텐츠에 대한 추가적인 정보를 제공하는 것이다. 한 예로 이미지를 만드는 경우 이 이미지가 만들어진 시간, 창작자 등과 같은 정보를 워터마크로 만들어서 이미지에 삽입하는 것이다.

### 5) Usage control

이것은 멀티미디어 컨텐츠를 복사하거나 재생하는데 특별한 하드웨어 장치가 필요한 경우, 디지털 워터마크가 컨텐츠에 삽입되어 컨텐츠를 복사할 수 있는 횟수 등을 제어하는데 워터마크를 사용하는 것이다. 이 방법의 경우 매번 카피가 일어날 때

마다 하드웨어가 워터마크를 수정하게 되므로 나중에는 더 이상 카피하지 않게 될 것이다.

### 2.3.4 디지털 워터마킹의 특성에 따른 기술 분류

가시성과 관련해 구분하는 방법 이외에도 그 응용 분야 및 용도에 따라 크게 Robust 워터마킹과 Fragile 워터마킹으로 구분할 수 있다.

#### 1) Robust 워터마크

우선 삽입되는 정보로 인해 원래의 저작물이 사람이 인지할 수 있을 만큼의 손상 및 품질 저하가 있어서는 안 되며, 저작권 정보가 되도록 여러 가지 공격(압축, 회전, 크기조절, 부분 삭제 등)시에도 검출되어야 하며, 인쇄나 스캐닝 시의 '디지털 아날로그 변환' 혹은 '아날로그 디지털 변환'에도 견딜 수 있어야 한다. 이렇게 저작권 정보를 끝까지 검출하게 보장함으로서 저작물에 대한 권리 표시를 할 가치 있는 컨텐츠에 적용된다. 이를테면 방송사의 방송물이나 음반 물에 적용될 수 있겠다.

하지만 아직까지 전 세계적으로 완벽하게 상기 기술한 외부공격에 100% 완벽한 방어를 할 수 있는 워터마킹 기술은 개발되지 못했다. 보안성이 높아지면 사용자 편의성이나 성능이 저하되게 되어 있다. Robust 워터마킹에서도 강인성을 높이기 위해 복잡한 embedding을 거치게 되면 detecting 시 많은 로드를 가지게 되는

위험성이 크다. 따라서 시장성 또는 상품성과 관련해서는 Robustness와 Complexity와의 상호 조율이 필요하다.

### 2) Fragile 워터마크

워터마크의 강인성을 통해 소유권 주장이나 저작권과 관련된 목적으로 사용된 것이 Robust 워터마킹이었다면 워터마크 자체가 아주 작은 외부 공격에도 깨지게 만들어 원본 여부를 감별해내는 것이 Fragile 워터마크이다. 따라서 워터마크가 검출되는 저작물은 위·변조가 진행되지 않은 원본임을 증명할 수 있게 해 '인증'과 '무결성'에 대한 증명을 하게 된다. 또한 워터마크 삽입기술에 따라 어느 부분이 위·변조되었는지 위치를 추적할 수 있게 하는 기능까지 추가할 수 있다.

### 3) Semi-fragile 워터마크

Robust와 Fragile의 중간 형태로서 일정 수준 이상의 변화에만 워터마크가 손상되게 하는 방법이다. 압축이나 코딩 등과 같은 경우는 비의도적인 공격으로 인식해 살아남고, Copy & Paste와 같은 의도적 공격에는 공격 위치를 확인할 수 있는 워터마크이다. 원본 필요 유무에 따라 Private 마킹, Public 마킹, Public Key 마킹 등으로 구분할 수 있다. Private 마킹은 워터마크 검출 시 원본 데이터가 필요하며, 검출 결과로 삽입되었던 마크를 출력해 입력한 마크와 삽입돼 있는 마크를 비교해 진위 여부를 판별한다.

Public 워터마킹은 원본 없이 워터마크 삽입에 사용된 Key만으로 검출을 시행해 삽입된 워터마크를 얻을 수 있는 방법이다. 원본 없이 키에 의존해 추출하기 때문에 Private 마킹에 비해 상대적으로 설계와 구현이 어렵다. 하지만 원본이 필요 없기 때문에 관리와 사용의 편의성은 높다.

Public Key 워터마킹은 가장 발전한 형태로 공개키 기반으로 삽입, 추출을 진행하는 방식이다. 즉 사용자의 비밀키로 워터마크를 삽입하며, 사용된 비밀키에 대응되는 공개키로 워터마크를 검증할 수 있다. 공개키 방식의 특성상 누구나 마크를 검증해 소유권 정보를 획득할 수 있으나 워터마크가 제거된 원본을 얻을 수 없어야 한다.

또한 워터마크가 공간영역에 삽입되는 Spatial영역과 주파수 영역에 삽입되는 Frequency 영역으로 나누어 볼 수 있다. 시간·공간 영역에 워터마크를 삽입하는 방식은 디지털 데이터에 직접 워터마크를 삽입하게 되는데 이럴 경우 변형이나 신호처리 기술에 의해 워터마크가 쉽게 깨지는 특성을 갖고 있기 때문에 주로 Fragile 워터마크 분야에 쓰이고 있다. 주파수 영역에 워터마크를 삽입하는 방식은 인간이 인지하기 힘든 주파수 대역으로 변환 후 변환 영역에서 삽입을 하게 된다. 시간·공간 영역에 워터마크를 넣는 것보다는 보다 강인한 성질의 워터마크를 특징으로 한다.

### 2.3.5 공간 영역에서의 워터마킹 방법

워터마크를 삽입하는 방법이나 응용 기술에 따라 데이터를 공간적 관점에서 삽입하는 방법(Spatial Domain Method)과 주파수 영

역에서 삽입하는 방법(Frequency Domain Method)으로 나눌 수 있다.

공간적 관점에서 워터마크를 삽입하는 방법은 이미지와 같은 데이터를 공간적 측면으로 분석하여 삽입하려는 정보를 공간상에서 흩어 버려서 쉽게 구별을 할 수 없도록 하는 방법으로, 일반적으로 화면 화소 값에 미세한 변화를 워터마크로 사용한다. 이 방법은 워터마크의 삽입은 쉽지만, 손실 압축이나 필터링과 같은 이미지 처리에 약하다는 면이 있다.

물리적 픽셀 영역, 즉 공간 영역에서 워터마크를 삽입하는 가장 간단한 방법은 픽셀들을 임의적으로 선택하여 밝기 값의 LSB(Least Significant Bit)를 변형시키는 것이다. 이 방법은 잡음과 일반적인 신호 처리에 강인하지 못하다는 단점을 가지고 있다. 또한 데이터 전송 및 잡음에 매우 민감하고, 데이터 압축과 같은 영상의 변형에 내장된 워터마크를 쉽게 손실하는 문제점이 있다.

이러한 단점을 극복하기 위해 인간의 시각 특성을 이용하게 된다. 즉 인간 시각의 마스킹 효과에 의해 영상 내의 Texture 영역이나 윤곽선 둘레의 밝기 값의 변화는 육안으로 잘 구별할 수 없다는 점을 이용하여 워터마크를 삽입한다.

다음은 공간 영역에서의 워터마킹 방법들이다.

### 1) Bender가 제안한 방법

공간 분석 방법 응용의 대표적인 예로서 Bender가 제안한 방법으로 패치워크(Patchwork)가 있다. 이 방법은 이미지에서 n개의 쌍을 임의로 선정한 (ai, bi)에서 ai는 명암 값을 하나씩 더해 주고,

bi는 명암 값을 하나씩 빼 줌으로써 공간상에 디지털 워터마크가 삽입하도록 구현하였다. 이 방법은 가시적인 이미지의 질을 저하시키는 단점이 있다.

### 2) Pitas와 Kaskalis가 제안한 방법

패치워크(Patchwork)와 유사한 방법으로서, Pitas와 Kaskalis의 논문에서 제안한 방법은 이미지를 두 개의 동등한 크기의 부분 집합으로 나누어 그 중 하나의 부분 집합에 있는 픽셀에 대하여 양의 정수인 k-factor를 더하는 방법을 제안하였다. 그러나 이미지의 각 픽셀의 명암을 모두 계산하기 때문에 데이터가 적은 흑백 이미지에서도 비효율적인 방법이다. 그러므로 데이터의 양이 매우 많은 칼라 이미지에 적용하기에는 불가능하다.

### 3) Caronni가 제안한 방법

Caronni의 논문에서는 픽셀 단위의 계산 량을 줄이기 위해서 이미지를 N의 블록으로 나누어 각 이미지 블록의 밝기 값에 비트 스트림(Bit Stream)을 삽입하는 방법으로 블록에 있는 픽셀의 평균값이 임계 값보다 클 경우에는 '1'로 부호화하고, 임계 값보다 작을 경우에는 '0'으로 부호화 하는 방법을 제안하였다. 그러나 이 방법 또한 칼라 이미지에서는 그 계산 량이 많아 블록이 클수록 워터마크가 손실되거나 원본 이미지의 질을 떨어뜨리는 단점이 있다.

### 2.3.6 주파수 영역에서의 워터마킹 방법

주파수를 이용한 방법은 멀티미디어 데이터를 주파수 성분의 아날로그 신호로 변환하고 삽입하려는 워터마크를 동일하게 아날로그 신호로 변환하여 삽입하는 방법이다. 일반적으로 데이터를 변환하는 방법으로 이산 코사인 변환(DCT : Discrete Cosine Transform), 고속 푸리에 변환(FFT : Fast Fourier Transform), 웨이블릿 변환(Wavelet Transform)등을 이용한다.

이러한 방법들은 삽입하려는 워터마크 계수들이 원래 데이터의 전 영역에 분포하게 되며 한번 삽입된 워터마크는 삭제가 어려운 장점이 있어 많이 사용되나, 알고리즘이 다소 복잡하며, 잡음과 압축 영상에 강하다.

주파수 영역에서의 워터마킹 방법은 영상 데이터를 Fourier Mellin, Fourier Transform, DCT(Discrete Cosine Transform), Wavelet등과 같은 변환으로 주파수 공간으로 변환하여 그 주파수 영역들 중에서 시각적으로 덜 민감한 부분에 적응적으로 워터마크를 삽입하는 방법이다.

다음은 주파수 영역에서의 워터마킹 방법 중 대표적인 방법들이다.

#### 1) Cox가 제안한 방법

Cox의 방법은 가장 널리 알려진 방법으로써, N×N 이산 코사인 변환 계수 중 가장 높은 n개의 이산 코사인 변환 계수의 함수에 의한 Sequence를 삽입하는 방법을 제안하였다.

Cox가 제안한 방법은 대역 확산(Spread Spectrum) 기법을 이용

한 방법으로, DCT변환을 통해 얻은 주파수 성분의 계수에 워터마크를 삽입함으로써 시각적으로 덜 민감한 고주파 성분에 적응적으로 워터마크를 삽입하였다.

대역 확산 통신에서는 협대역 신호를 훨씬 큰 대역폭에 걸쳐서 보냄으로써 하나의 주파수에서 볼 때 신호의 에너지는 아주 적은 양이 된다는 개념으로 워터마크를 주파수 성분에 걸쳐서 분산시켜 삽입함으로써 에너지가 분산되어 한 주파수에서 보면 매우 적은 양이 훼손이 어렵게 되기 때문에 워터마크가 삽입된 주파수의 위치나 내장 정보를 알 수 없게 만드는 것이다. 삽입에 이용되는 주파수 성분도 원본 영상의 특성을 결정짓는 성분들이 선택되므로 각종 신호 처리 과정이나 고의적인 공격 등에 대하여 강인한 특성을 갖게 된다.

워터마크 삽입 방법에서는 원본 영상의 전체 크기에 대한 DCT를 수행한 후 DC성분을 제외한 주파수 계수 중에서 가장 큰 값을 가지는 주파수 계수를 선택하여 워터마크를 삽입하였다.

그러나 이러한 대역 확산 기법은 공격에는 강하나 워터마크 삽입 후 화질의 변화가 생기고, 화질의 변화를 없애기 위해 중간 주파수에 삽입을 하면 화질은 좋은 반면 공격에 약한 경향을 보인다.

### 2) Boland가 제안한 방법

Cox의 방법과 비슷한 접근 방법으로 Boland 는 이미지를 블록으로 나누고, 이 블록내의 각 픽셀 값에 대한 편차를 구하며, 그 편차를 -127에서 127까지 정규화(Normalize)를 시킨 다음, 주파수 공간에서 계수들에 이진수를 삽입하는 방법을 제안하였다.

### 3) Podilchuk과 Zeng이 제안한 방법

인간의 시각 기관 구조의 특성을 이용한 Podilchuk 와 Zeng이 제안한 방법은 어느 정도 개선된 방법이다. 그러나 저작자가 이 방법을 시용할 경우 가시적인 변화로 인해 사용하기 어렵다. 또한 워터마크 감지의 경우 삽입 방법과 정확히 일치하는 과정을 통해서만 추출이 가능하다.

### 4) Xia가 제안한 방법

영상을 웨이블릿 변환한 후 최저주파 대역을 제외한 나머지 부대역에 워터마크를 삽입하는 방식을 제안한 Xia는 영상을 다해상도 분해하여 단계별로 다른 가중치를 주어 워터마크를 삽입하면 성능을 향상시킬 수 있다고 한다.

그러나 Xia가 제안한 방법은 워터마크가 삽입된 영상을 손실 압축시킬 경우 고주파 성분의 정보들은 손실되고, 저주파 성분의 정보들은 남아 있게 되므로 고주파 성분해서 추출한 워터마크는 손실이 된다는 특성을 갖고 있기 때문에 압축 영상에서의 워터마크 추출에 약한 단점을 가지고 있다.

# 3 장 Watermarking 실험

## 3.1 Ingemar J. Cox가 제안한 Watermarking 구현

### 3.1.1 Cox가 제안한 Watermarking 이론

Watermarking을 하고자 하는 원본 이미지를 $S_o$ 라고 하고 넣고자 하는 Watermarking을 $W$로 정의하고, 원래의 이미지$S_o$을 인자로 하는 함수 값을 $f(S_o, W)$라고 할 때 함수 값을 원래의 이미지에 더한 것을 Watermarking 이론이라 할 수 있다. Watermarking된 이미지 $S_w$을 식으로 표현하면 식 3.1과 같다.

$$S_w = S_o + f(S_o, W) \qquad \text{(식 3.1)}$$

이 이론에서 함수 $f$ 는 임의로 선택되는 것이지만, 강인성을 보장하려면 제약을 두어 결정하게 된다. Watermarking 한 가지 요구사항은 강인하게 하기 위해 임의의 노이즈를 첨가해야만 한다는 것이다.

만약 Watermarking 시그널을 원본 이미지와는 관련이 없는 별개로 만들려 한다면 Watermark 시그널 $f$ 는 $f(W)$가 될 수 있다. 이때는 Watermarking할 정보 $W$외에 워터마크를 만들 것이 없으므로 $W$을 워터마크 이미지로 사용할 수도 있다. 수식으로 표현하면 식3.2와 같다.

$$S_W = S_o + f(W) = f_o + W \qquad \text{(식 3.2)}$$

Watermarking된 이미지 $S_W$ 는 여러 곳을 거치면서 내용의 일부가 변경 되거나 훼손되는 상황을 맞을 수 있다. 이때 이를 유발하는 작업을 n이라고 한다면 작업 n은 일반적으로 원래의 이미지에 따라 나오는 결과가 좌우되는 경우가 많다. 따라서 n은 이미지 $S_o$ 을 함수 $n(S_o)$로 할 수 있다. 그러므로 Watermarking된 이미지 뷰어 프로그램으로 눈으로 보려할 때, 보려고 하는 대상 이미지는 $S_W$ 가 작업 n에 의해 약간은 다른 이미지 $S_W'$ 가 된다.

많은 디지털 Watermarking 방법들은 기본적으로 이상과 같은 수식을 기본 개념으로 하여 원래의 이미지에 워터마크를 삽입하고 새 이미지를 만들어내는 방식을 택하고 있다. 이 방법들은 크게 다음 두 가지의 상황을 고려하고 있다.

표 3.1 Watermarking의 방법

| Watermarking의 방법 | 수식 |
|---|---|
| 원래의 이미지와는 무관하게 Watermarking 시그널을 만드는 경우 | $S_w = S_o + W$ |
| Watermarking시킬 정보와 원래의 이미지를 가지고 만드는 경우 | $S_w = S_o + f(S_o, W)$ |

첫 번째 경우, 즉 원래의 이미지와는 무관하게 워터마킹 시그널을 만들 경우에는 워터마킹 정보를 시각 필터링(Perceptual Filtering)을 거쳐서 원래의 이미지 안에 은닉시킬 수 있는 형태로 만든 다음 원래의 이미지와 결합해 워터마킹된 이미지를 만들게 된다.

두 번째 경우, 즉 원래의 이미지와 워터마킹 정보를 결합해 워터마킹 시그널을 만들 경우에는 시각필터링을 거쳐서 나온 시그널과 원래의 이미지를 비선형 결합(Nonlinear Combination) 시켜 원래의 이미지에 워터마킹을 취하는 형태가 된다.

Cox는 워터마킹 시그널에 가중치 a를 두어서 워터마킹을 수행하는 방법을 제시했다. 이 상황을 수식으로 쓰면 식 3.3과 같다.

$$S_W = S_o(1 + aW) \qquad \text{(식 3.3)}$$

이 방법의 장점은 이미지가 특정한 주파수 채널에서 해상도나 선명도가 강조되거나 줄어들 때, 그에 따라서 워터마킹 정보도 같이 비중이 변할 수 있다는 점이다.

디지털 워터마킹의 용도로 멀티미디어 데이터의 원저자를 규명하는 것 이외에 디지털 워터마킹의 용도로 콕스는 로열티 지불여부를 알아내기 위한 광역 모니터링 (Broadcast Monitoring to Determine Royalty Payments), 인증(Authentication) 등을 제시하고 있다. 로열티 지불여부를 알아내는데 디지털 워터마킹이 쓰일 수 있다는 것은 디지털 워터마킹된 이미지들을 복사해 간 모든 사람들의 위치를 전부 파악한다는 점을 염두에 둔 개념이다.

### 3.1.2 디지털 워터마킹의 요건

#### 1) 워터마크의 손실

일단 가장 중요한 사항으로, 디지털 워터마킹이 원래의 데이터에 포함되었는지를 쉽게 알아볼 수 없도록 워터마킹이 구현돼야 한다. 또한, 워터마킹이 포함됨으로 인해 원래의 데이터의 품질에 이상이 생기는 일이 없어야 한다. 이에 대해서는 아직도 기술적으로 해결해야할 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 논의대상이 될 수 있다.

### 2) 시그널의 일반적인 일그러짐에 대해 견고함이 유지

손실압축을 비롯하여 멀티미디어 데이터들은 많은 손실요소로 인해 원래의 데이터에서 시그널들이 일그러질 수 있는 경우를 많이 포함하고 있다. 이미지의 선명도를 높인다거나, 색상의 일부를 바꾼다거나, 또는 오디오 시그널의 베이스 주파수를 증폭시킨다거나 할 때, 데이터 안에 있는 워터마킹이 깨지지 않고 유지될 수 있는가, 또한 워터마크를 읽을 수 있는 뷰어가 이렇게 변경된 데이터 안에 있는 워터마크를 읽어낼 수 있는가가 워터마킹의 중요한 이슈가 될 수 있다.

### 3) 워터마크를 없애기 위한 시도에 대처

받아온 멀티미디어 데이터에 워터마크가 포함돼있다는 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 시그널을 찾아서 없애려는 시도가 있을 수 있다. 이때 이를 방지할 수 있는 매커니즘이 있어야 할 것이다.

### 4) 응용 프로그램을 위한 적당한 데이터

워터마크 시그널 안에 포함될 수 있는 정보의 양도 워터마킹에서 중요한 이슈가 된다.

### 5) 워터마크를 변경하거나 계속 추가 가능

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 거쳐 갈 때 각각 워터마크를 추가해 원래의 데이터가 어떤 경로를 거쳐 배포가 되었는지를 파악하게 할 수 있을 것이다. 이점에 대해서도 고려할 것들이 많이 있다.

### 6) 워터마크의 확장이 용이

새로운 워터마킹 알고리즘을 만들어 기존 것을 대체할 것이 아니라 기존의 워터마크를 확장함으로 더욱 강력한 워터마킹을 수행할 수 있게 해야 한다.

## 3.2 Watermarking 실험

### 3.2.1 실험 시스템 환경

본 논문에서 워터마크 삽입 및 추출하는 과정을 구현함에 있어서 펜티엄 III 450MHz의 CPU의 시스템과 Windows 2000 Server운영체제를 이용하였다. 자세한 환경은 다음과 같다.

표 3.2 시스템 실험 환경

| 구 분 | 내 용 |
|---|---|
| CPU | Intel Pentium III 450 MHz |
| Main memory | 512Mb |
| 운영체제 | Windows 2000 Server |
| 응용프로그램 작업환경 | Win32 |
| 사용 언어 | C언어 |
| 개발 도구 | Microsoft Visual C++ 7.0 |

### 3.2.2 실험 방법

영상의 디지털 워터마킹을 실험하기 위해서 첫 번째로 랜덤함수에 의한 임의의 숫자로 구성된 서명(Signature)파일을 만들게

된다. 이 임의의 숫자는 이미지 파일에 사람의 눈으로 식별하기 어렵도록 첨부가 된다. 서명이 첨부된 이미지에서 다시 워터마크를 추출한 후 원래의 서명 파일과 비교하여 워터마킹의 성능의 측정 실험을 하였다.

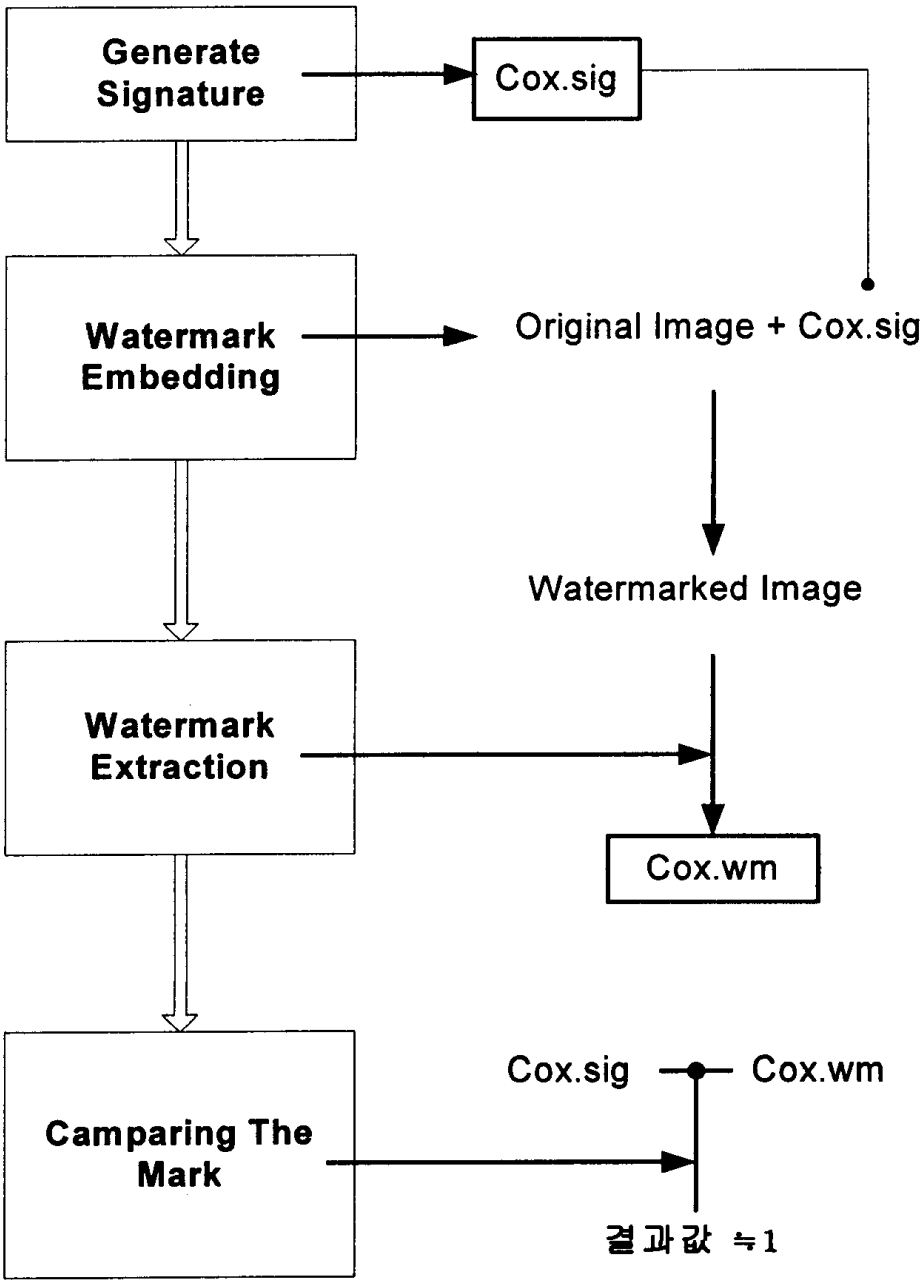



그림 3.1 cox의 워터마킹 증명 흐름도

### 3.2.3 서명 생성

Watermark 삽입과 추출을 하기 위해서는 가우시안 분포에 의한 임의의 숫자와 파라미터를 생성해야만 한다.

가우시안 분포는 모든 과학에서 가장 보편적이고, 많이 쓰이는 분포이다. 특히 실험오차에 대한 측정은 일반적으로 이 확률분포를 따른다. 가우시안 분포는 종종 실제 분포에 아주 근사를 보인다. 가우시안 분포는 다음 식3.4와 같이 주어지는 밀도를 이용한 연속적이면서도 대칭적인 분포이다.

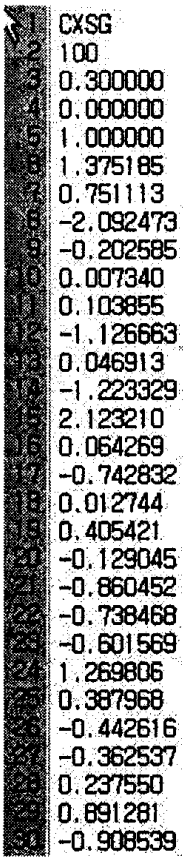
$$P(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \qquad \text{(식 3.4)}$$

여기서 $\mu$는 평균이고 $\sigma^2$은 분산이다. 균일 랜덤 변수는 주어진 상한값과 하한값이 있는 반면에 가우시안 랜덤 변수는 그러한 경계가 없다.

```
//#define RAND_MAX 0x7fff -> stdlib.h
x1 = 2.0 * ((random() & RAND_MAX) / ((double) RAND_MAX + 1.0)) - 1.0;
x2 = 2.0 * ((random() & RAND_MAX) / ((double) RAND_MAX + 1.0)) - 1.0;
x = x1 * x1 + x2 * x2;
```

그림 3.2 임의의 숫자 생성

명령 gen_sig.exe -o cox.sig으로 생성된 서명(Signature)파일은 다음과 같다.




중략

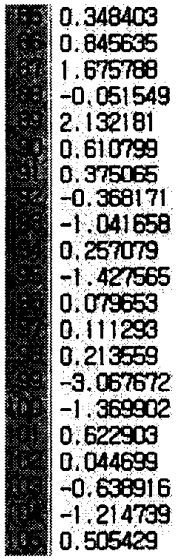



그림 3.3 생성된 서명 (Signature) cox.sig 파일

### 3.2.4 Watermark 삽입

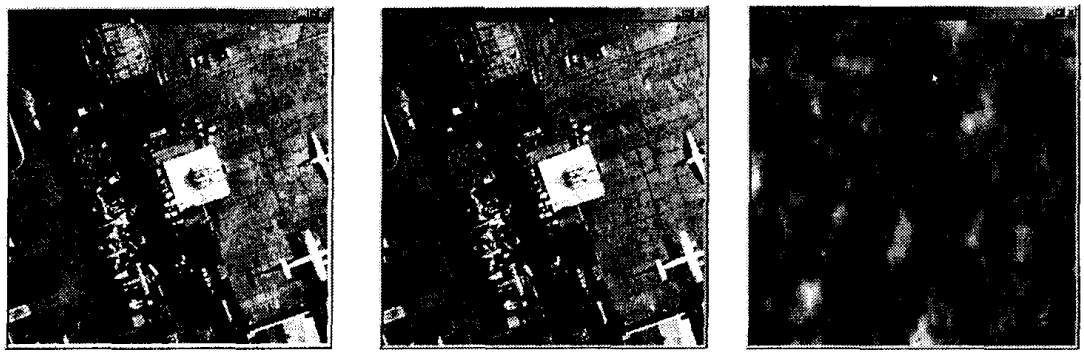
서명 파일은 특별한 watermark 삽입된 장점을 얻기 위해 분석하는데 사용된다. 실험에 사용된 영상의 포맷은 256색상의 PGM(Portable GrayMap)을 이용하였다. 영상을 8X8 블록으로 나누어 DCT함수를 이용하여 변환한 후, 주파수 성분중 가장 큰 값에 임의의 숫자를 삽입한다.

```
for (row = 0; row < rows; row++)
  pgm_writepgmrow(out, output_image[row], cols, maxval, 0);
```

그림 3.4 Watermark 삽입

pgm_writepgmrow함수는 NetPBM[29]의 libpgm2.c 에 정의되어있다. 함수에서 out 인자는 output 파일의 포인터이고, output_image[row]는 이미지에 대한 gray row에 대한 포인터이다. cols는 이미지에 대한 세로줄이고 maxval은 gray 값에 대한 최대 값이며, 0은 pgm.h에 정의된 forceplain 정수값이다.

원래의 이미지에 생성된 서명파일을 더하여 워터마킹된 이미지는 사람의 육안으로 식별하기 어렵고 파일 크기의 변화는 없거나 약간의 차이만 있었다.



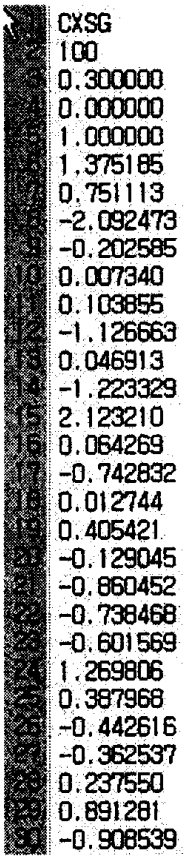
<워터마크 삽입 전> <워터마크 삽입 후> <변형된 부분>

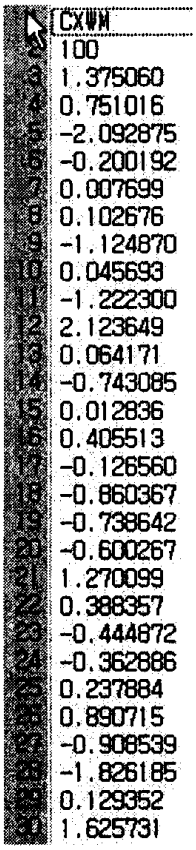
그림 3.5 워터마킹 이미지 비교

### 3.2.5 Watermark 추출

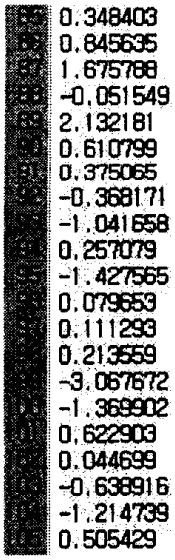
삽입된 마크를 추출하기 위해서는 서명이 삽입되기 전 원래의 이미지와 서명이 필요하다. 서명과 이미지의 계산에 의해 서명이 삽입된 이미지에서 워터마크를 추출해 내어 텍스트 파일로 저장하면 된다. 이미지 파일을 DCT 변환을 한 후, 주파수 계수 중에서 가장 큰 값을 가지는 주파수 계수를 선택하여 추출해 낸다. 원래의 이미지를 original.pgm이라고 하고 워터마크가 삽입된 이미지 파일을 wm.pgm이라고 하고, 추출할 파일명을 cox.wm로 할때 다음과 같은 명령으로 워터마크 파일을 추출한다.

```
cox_d -s cox.sig -i original.pgm -o cox.wm wm.pgm
```

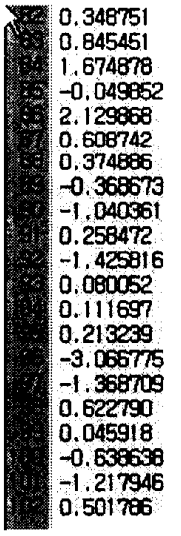



중략




cox.sig 파일




cox.wm 파일

그림 3.6 서명 파일과 추출한 워터마크 파일

### 3.2.6 서명 파일과 추출 파일 비교

최종 단계는 추출된 파일과 원래의 서명 파일을 비교하는 것이다. 결과는 보통 상관 계수이다. 원영상과 워터마킹된 영상의 차이를 구한 후에 워터마크와의 상관관계를 구하여 워터마크를 확인한다. 결과 값이 0에 가깝다면 마크가 검출되지 않았다는 뜻이고 1에 가까울수록 정확하게 마크가 검출된 것이다.

```
s1 += sig_x * in_x;
s2 += in_x * in_x;
s3 += sig_x * sig_x;

fprintf(out, "%f\n", s1 / sqrt(s2 * s3));
```

그림 3.7 서명 파일과 추출 파일 비교 결과 계산

서명 파일을 읽어들여 정수 sig_x에 넣고, 워터마크 파일을 읽어들여 정수 in_x에 삽입한다. 읽어들인 값을 각각 그림 3.7과 같이 곱셈하여 s1, s2, s3에 각각 삽입한 후 s1 / sqrt(s2 * s3)를 계산하여 출력한다.

### 3.2.7 실험 결과 및 분석

이미지의 크기에 따른 결과 값을 비교분석하였다. 결과는 PGM파일의 픽셀의 크기가 크고 용량이 많을수록 상관계수의 값은 작게 나타났다.

표 3.3 이미지 크기에 따른 결과 값

| 크기(Pixel) | 파일명 | 용량(byte) | 결과 값 |
|---|---|---|---|
| 512 × 512 | air.pgm | 262,263 | 0.998661 |
| | couple.pgm | 262,202 | 0.999277 |
| 256 × 256 | house.pgm | 65,551 | 0.999984 |
| | pattern.pgm | 65,551 | 0.999999 |

결과 값이 0.2 이상으로 검출될 경우에 워터마크가 훼손되지 않고 보존 되었다고 할 수 있다.

실험에 사용된 이미지에 대한 이미지 보존율을 알아보기 위해 PSNR(Peak Signal to Noise Ratio)를 구해보았다. PSNR이란 복원 영상의 객관적인 화질평가를 나타낸다. PSNR이 높을수록 원본 이미지의 보존율이 높다는 것을 의미한다.

표 3.4 이미지 크기에 따른 PSNR 값

| 크기(Pixel) | 파일명 | PSNR(dB) |
|---|---|---|
| 512 × 512 | air.pgm | 28.452227 |
| | couple.pgm | 27.968572 |
| 256 × 256 | house.pgm | 23.162318 |
| | pattern.pgm | 27.303378 |

결과적으로 이미지의 크기가 클수록 원본 이미지의 보존율이 큰 반면 워터마크의 검출이 상대적으로 어려웠다.

# 4장 결 론

멀티미디어 산업의 비약적인 발전에 의해 데이터의 디지털화가 급속히 증가하였고, 디지털 데이터의 장점인 복제 및 변조가 쉬운 점을 이용하여 불법 복제 및 배포가 확산됨에 따라 지적 소유권 문제가 크게 부각되었다. 이러한 디지털 데이터의 소유권을 효과적으로 보호하기 위해 디지털 워터마킹이 연구되었다.

본 논문에서는 주파수 영역에서의 워터마킹 중에 DCT (Discrete Cosine Transform) 방법을 이용한 Cox 방식을 이용하여 실험하였다. 공간영역에서의 워터마킹은 변환 식을 사용하지 않고 영상의 화소 값을 직접적으로 변화시켜 워터마크를 삽입하는 방법이기 때문에 영상 변형이나 잡음 등의 공격에 약하지만 주파수 영역의 방법은 DCT(Discrete Cosine Transform), DFT(Discrete Fourier Transform), DWT(Discrete Wavelet Transform) 등의 변환 식을 이용하여 워터마킹을 삽입하여 공격에 강한 특징을 가지고 있다. 실험한 결과는 원본 이미지의 크기가 클수록 이미지 보존율은 좋았으나, 워터마킹 검출은 어려웠다. 보안성을 높이게 되면 원본의 이미지의 손상을 가지게 되고 탐지(Detecting)시에 많은 로드를 가지게 되고 그 반대의 경우에는 삽입(Embedding)이 쉽게 노출되는 위험을 가지게 된다. 상품성에 따라 강인성(Rubustness)과 복잡성을 적당한 값으로 조정이 필요하게 된다. 향후 이미지의 크기와 복잡성에 따른 적당한 대역의 주파수를 결정하여 Detecting 할 때 로드를 줄이고, 원본 이미지를 밝혀내는데 가장 성능이 좋은 Watermarking 기법이 연구되어져야 한다.

# 참 고 문 헌

[1] 미디어 웍스 http://www.mediaworks.co.kr/WindowsMedia Technology

[2] 김진영, 실트로닉 http://www.sealtronic.com/html/library/l_1.html 월간지 디지털 컨텐츠 보안 기술연재

[3] 마이크로소프트 http://www.microsoft.com/koreawindows/windowsmedia

[4] 이광수, 과학기술원 논문, 디지털 워터마킹 방법을 이용한 디지털 미디어 컨텐트의 저작권 보호방법 2001

[5] 최운종, 건국대학교 대학원, 영상의 소유권 보호를 위한 웨이브릿-기반 디지털 워터마킹 방법, 2001

[6] 최재곽, 경일대학교, 디지털 컨텐츠 보호 기술, 2001

[7] 이광수, 과학기술원, 디지털 워터마킹 방법을 이용한 디지털 미디어 컨텐트의 저작권 보호방법, 1998

[8] 한재혁, 박원배, 안재형, 충북대학교, Hybrid 디지털 워터마킹, 2001

[9] 전종민, 성균관대, 디지털 컨텐츠 인증 및 저작권 보호를 위한 워터마킹과 실용적인 분배 프로토콜에 관한 연구, 2001

[10] 김원겸, 충남대, 멀티 미디어 데이터의 저작권 보호를 위한 Digital Watermarking 기법, 2001

[11] 황영선, 성균관대 정보통신 대학원, 디지털 콘텐츠 산업의 구조적 분석 및 개발 방안에 관한 연구, 2001

[12] 한국인터넷정보센터, 인터넷 이용자 수 및 이용행태 조사, 2002

[13] 한국인터넷정보센터, 2002년 8월 인터넷 통계 월보, 2002

[14] 한국 인터넷 방송 협회, http://www.korwa.or.kr/korean/what/what01/what02.asp?ttable=middletable&b_id=11

[15] 이신주, 정성환, 창원대 정보통신 연구소 논문집, 저작권 보호를 위한 워터마크 기술, 2001

[16] 김영식, 서강대, 웨이블릿 영역에서의 디지털 영상 워커마킹 방법, 1999

[17] 석종원, 홍진우, ETRI 방송기술 연구부, 워터마크를 이용한 멀티미디어 컨텐츠의 저작권 보호,

[18] 영상의 DCT 변환 영역에서의 워터마크 삽입기술, 고수창, 울산대학교, 1998

[19] 이정수, 김회율, 방송곡학회논문지 1998년 제 3권 제 2호, 영상 정보의 소유권 보호를 위한 Watermarking 기술의 개발, 1998

[20] 한국전자통신연구원 http://www.etri.re.kr/report/network.html

[21] 인터넷 정보센터 http://stat.nic.or.kr/stat_report.html

[22] 마이크로소프트 http://www.microsoft.com/koreawindows/windowsmedia/wm7/drm/architecture.asp

[23] Knuth, D., The Art of Computer Programming, 1997

[24] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal G. Shamoon, Secure spread spectrum watermarking for multimedia, 1997.

[25] Ingemar J. Cox, http://www.neci.nj.nec.com/homepages/ingemar/ingemar.html

[26] Stirmark benchmark Site http://www.cl.cam.ac.ur/~fapp2/watermarking

[27] Digimarc Site http://www.digimarc.com

[28] SDMI http://www.sdmi.org

[29] Tomas Sander, Security and Privacy in Digital Rights Management, 2001

# Abstract

Prevailing of digital contents industries has brought a rise of interest in Digital Rights Management(DRM) technology. In the era of analogue, we could have controlled illegal uses and duplications of contents by the related laws and regulations; however, after they have been transformed digitally laws and regulation have carried no legal binding forces.

Thus, the demand of protective systems have been proposed which can prevent illegal uses and duplications fundamentally. This brought studies of DRM technology.

I have examined Digital Watermarking, especially in the range of signals proposed by Ingemar J. Cox. Even though huge image files were hard to be analyzed out, PSNRs(Peak Signal to Noise Ratio) was showed at high.