디지털 컨텐츠의 저작권 관리를 위한 워터마킹 기술

Watermarking for Digital Rights Management

정사라(S.R. Jung) 음향기술연구팀 연구원
석종원(J.W. Seok) 음향기술연구팀 선임연구원
홍진우(J.W. Hong) 음향기술연구팀 책임연구원, 팀장

본 논문에서는 현재 표준화 진행중인 디지털 저작권 관리 시스템의 다양한 기술들을 살펴본다. 저작권 관리 시스템을 구성하는 요소로 암호화, 접속 제한, 복사 제어, 신원 확인 등이 있으며 이러한 요소를 이루는 기술로 최근 워터마크의 연구가 활발히 진행중이다. 워터마크 기술은 응용 범위가 넓고 잠재적 개발 가능성이 크지만 아직까지 분명한 한계가 있으며, 강인성과 품질 사이에 요구사항이 서로 트레이드 오프 상태에 있는 단점이 있다. 따라서 저작권 관리 시스템의 구현을 위해서는 먼저 시스템의 요구사항을 분명히 규정하고, 그것에 적합한 기술을 최적화하는 것이 필요하다.

I. 서 론

현재 전자상거래 시장은 급속한 성장을 하고 있다. 소비자 중심의 전자상거래에서 디지털 미디어의 유통은 매우 중요한 역할을 담당한다. 한 예로 MP3 디지털 음악은 선풍적인 인기를 끌고 있으며, 그 외에 비디오 스트리밍이나 디지털 북과 같은 다른 형태의 미디어들도 시장에서 점차 중요한 위치를 차지해 가고 있다. 한편, GPRS(General Packet Radio Service)나 UMTS(Universal Mobile Telecommunications Service) 등의 2세대, 3세대 이동통신망의 개발은 고정된 위치의 이용자들뿐만 아니라 사용자가 어디에 있든 인터넷과 디지털 미디어를 빠르게 접속할 수 있는 환경으로 이끌게 되었다.

디지털 미디어와 그 유통이 활발하게 이루어지면서 컨텐츠 제작자에게 디지털의 완벽한 복제 특성은 심각한 걱정거리로 불거졌다. 컨텐츠 제작에는 많은 비용과 노력이 필요하므로 불법 복제물의 유통은 저작권자에게 심각한 경제적 손실을 입히게 된다. IIPA (International Intellectual Property Alliance)는 미국 영화산업과 음반산업의 해적판에 의한 손실이 각각 연간 미화 13억 달러, 17억 달러에 상당함을 추정하였다[1].

질이 좋은 컨텐츠를 정당하게 대우하고, 소유권을 보호하려면 디지털 미디어 유통 과정에서 저작권 보호 기능을 포함해야 한다. 멀티미디어 데이터에 대해 접속을 제한하고 제어하는 디지털 저작권 관리(Digital Rights Management: DRM) 시스템은 일반적으로 암호화, 접속 제어, 키 관리 등으로 이루어져 있으며 대다수가 복제 방지, 지불 인터페이스 등을 포함한다. 그러나, 실제로 복제 방지나 제어를 구현하기는 매우 어려워서 저작권 보호의 마지막 방어선으로 개별 복사본에 대한 사용자 확인, 역추적이 제안되었다. 이것은 컴퓨터 소프트웨어의 일련번호

와 비슷한 것으로 복제를 막을 수는 없지만 해적판의 소스를 밝혀내는 데 도움을 줄 수 있다. 데이터 신원 확인과 복제 제어를 위한 DRM 시스템의 주요 기술로서 최근에 디지털 워터마킹 기술이 부각되고 있다.

본 고에서는 DRM을 위한 워터마킹의 필요성을 소개하고, 최근의 DRM 표준화에 관한 노력을 살펴본다[2],[5]. 또 워터마킹에 사용된 다양한 기술들과 그 한계를 서술하고 마지막으로 결론을 맺는다.

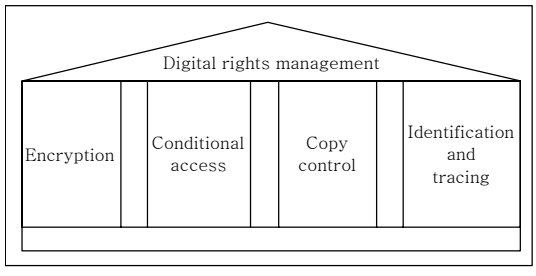
II. 멀티미디어에 대한 저작권 관리 (DRM)

DRM이란 디지털 컨텐츠에 대한 지적재산의 교환이 안전하게 이루어지도록 관리하는 시스템이다. 즉 인터넷이나 이동망과 같은 온라인 또는 CD, 디스크와 같은 오프라인 상에서 디지털 형태의 음악, 비디오, 문서 등에 대한 저작권자의 권리를 효율적으로 보호하기 위한 방법이다. 따라서, DRM이 체계적으로 수행될 경우 컨텐츠 소유주가 인증된 사용자에게만 안전하게 데이터를 유통시키고, 전체 유통 경로를 제어할 수 있게 해 준다. DRM을 구성하는 요소는 다음과 같다.

- 암호화: 허가 받지 않은 접속을 막기 위해 컨텐츠 전체 또는 부분을 암호화한다.
- 복호화 키 관리
- 접속 제어(조건부 접속): 어떤 사람에 대해 특정 기간, 특정 횟수로 접속을 제한할 수 있다. 예를 들어 데이터에 대한 초기접속은 무료지만, 그 후의 접속은 지불을 필요로 하게 할 수 있다.
- 지불 인터페이스: 미디어 유통에 관한 대부분의 비즈니스 모델은 금전 거래를 포함하고 있으며, DRM 시스템은 그러한 거래를 성립시킬 수 있어야 할 것이다.
- 복제 제어와 방지: 복사불가/1회가능/몇회가능/무한복사 등의 복사 제어와 복사본 복사의 저작권 형성 등을 다룬다. 복사 제어는 구현하기 매우 어려우며, 워터마킹과 같은 복잡한 기술을 필요로 한다. 워터마킹에 대해서는 뒤에서 자세하게 다룬다.
- 신원 확인과 역추적: 대개 멀티미디어 데이터의 출력 형태는 아날로그이므로 이것을 이용해서 복사본을 만들 수 있다(예로, 오디오 트랙의 스피커 출력이나 비디오 디스플레이 등을 들 수 있다). 이러한 종류의 복사를 방지하기란 거의 불가능하므로 필요할 경우, 아날로그 형태에서 디지털 복사본으로의 역추적과 신원 확인을 하게 된다. 이것은 데이터의 디지털 워터마킹(전자지문)으로 가능하며 이 기능 역시 DRM에 속한다.

(그림 1)에 DRM의 구성 요소를 나타내었다[2]. 다른 암호화 시스템과 마찬가지로 DRM 시스템의 강인성은 시스템을 구성하는 요소 중에서 가장 약한 요소의 강도에 의해 결정된다.

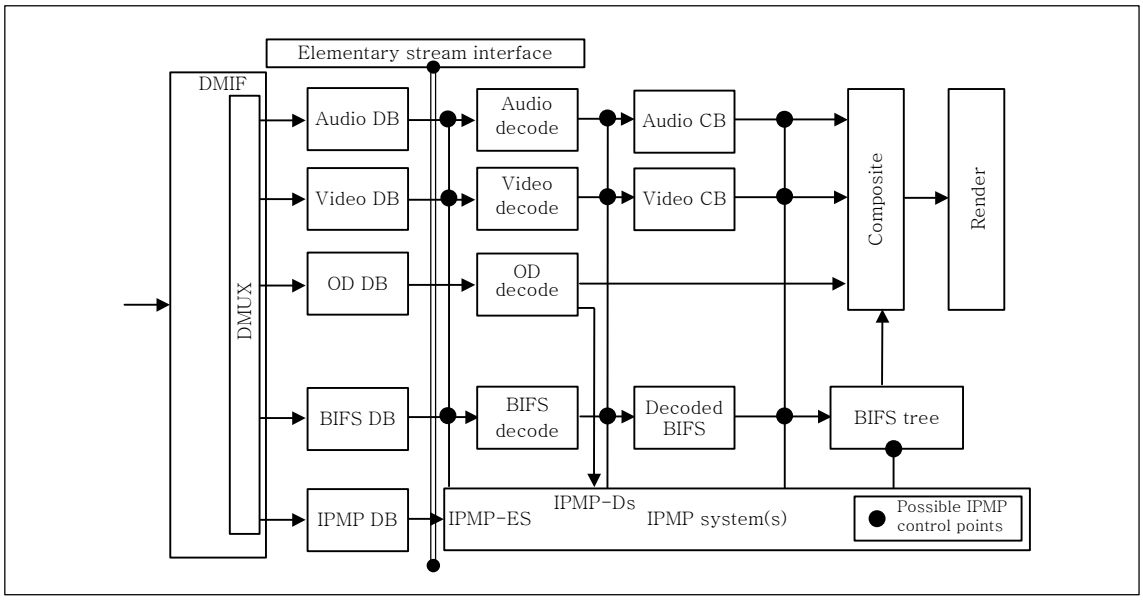
현재 DRM의 필요성은 널리 인식되었으며, 그에 따른 표준화 작업과 기존 방식의 보완이 활발하게 이루어지고 있다. DRM을 연구하는 주요 표준화 단체로 MPEG과 SDMI(Secure Digital Music Initiative), DVD/CPTWG(Copy Protection Technical Working Group), OPIMA(Open Platform Initiative for Multimedia Access), DVB(Digital Video Broadcasting), DAVIC(Digital Audio-Visual Council), 블루투스 특별 인터넷 그룹, TV-anytime, W3C 등을 들 수 있다.



(그림 1) DRM 구성 모델

1. MPEG-4 IPMP 표준화

ISO/IEC(International Electrotechnical Com-

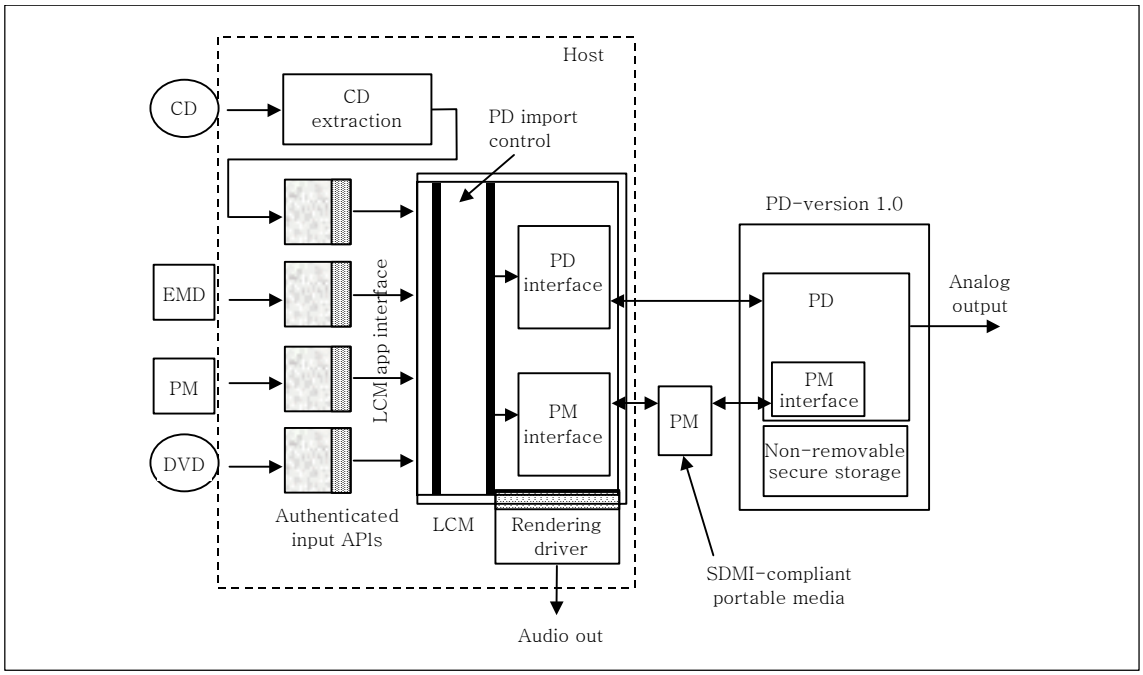


(그림 2) ISO/IEC 14496 단말에서 IPMP 프레임 구조

mission) 14496(일명 MPEG-4)에서는 IPMP (Intellectual Property Management and Protection)에 관한 프레임을 표준화하고 있다[3]. 기본 개념은 시스템에 '후크(제어 지점)'를 걸어서 DRM 시스템을 덧붙인 후 전체 시스템을 단단하게 죄이는 형태이다. 일반적으로 컨텐츠들은 암호화된 용기에 담겨 있거나 스트리밍 어플리케이션일 경우 실시간으로 암호화된다. 복호화 키와 사용 규칙은 어플리케이션의 요구사항에 따라 용기에 담겨 있거나 따로 분배될 수도 있다. MPEG-4의 미디어 객체들은 모두 그에 따른 메타데이터인 ODs(Object Descriptors)를 갖는데 이 ODs의 한 부분으로 IPMP-Ds가 있다. IPMP-Ds는 저작권 관리에 관한 정보를 갖는다. 특정 객체가 아닌 일반적인 DRM 정보는 IPMP-Ess(Elementary Streams)에 포함되어 있다. 이러한 IPMP-Ds와 IPMP-ESs가 IPMP 시스템과 MPEG-4 단말간의 통신 채널 역할을 하게 된다. 어떤 어플리케이션에서는 여러 개의 IPMP 시스템을 사용할 수도 있다.

(그림 2)의 MPEG-4 IPMP 시스템에서는 다양한 종류의 '후크'를 볼 수 있다. 역다중화기와 스트림 복호화기 사이에서 대부분의 제어가 이루어지는데, 복호화된 이후의 컨텐츠에 대해서 제어할 수도 있다. 예를 들어 컨텐츠 부호화 전에 삽입한 워터마크는 컨텐츠 복호화 이후에야 추출이 가능하다. 일반적으로 '후크'는 암호의 복호화 과정에서 워터마킹에 이르기까지 다양한 과정이 가능하며 실질적인 처리는 IPMP 시스템에서 이루어진다.

MPEG-4 IPMP 시스템의 작동 예는 다음과 같다. 먼저 고객의 시스템이 초기화된다. 이것은 BIFS (audio-visual scene description), ODs, 그리고 IPMP-ESs의 초기화를 의미한다. 고객이 가진 DRM 시스템은 서버와 고객간에 암호 관계를 성립하고 유지하도록 퍼블릭/프라이비트 키를 포함하고 있다. 고객이 서버에 MPEG-4 장면의 전송을 요구하면, 안전한 채널을 만들기 위해 고객과 서버는 양방향 인증 프로토콜을 수행한다. 이 때 인증의 한 부분으로 세션 키를 교환하며, 일단 채널이 성립되면 세션 키로 암호화된 복호키와 다른 요구 정보들이 전송된다. 이 키들은 IPMP-ESs로 옮겨진 후, 컨텐츠와 매핑한다. 이 매핑은 각 컨텐츠에 해당하는 IPMP-DSs를 이용하여 이루어지며, 이후 컨텐츠의 복호키를 추출한다. 모든 키들의 교환과 추출이 끝나면, 스트림 관리자는 어떤 컨텐츠 스트림을 보호할 것인지



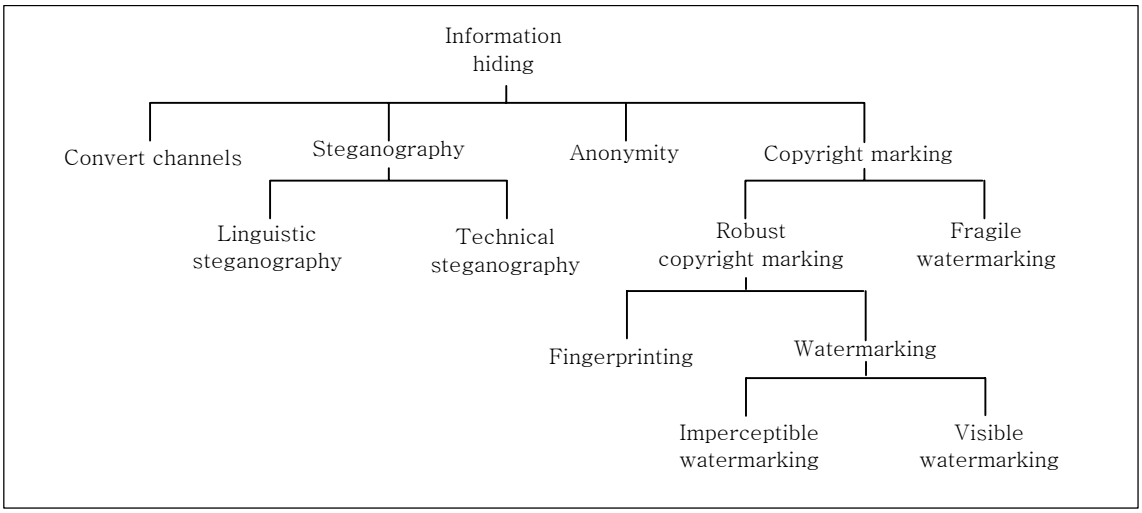
(그림 3) SDMI 휴대용 장치 구성의 개념도

결정한다. DRM 시스템은 이 스트림에 관계된 IPMP-DSs를 조정하여 사용 규칙들을 찾아내고, 컨텐츠 복호화를 수행한다.

2. SDMI 휴대용 장치 규격

SDMI는 오디오 DRM의 공개 표준을 제정하기 위한 산업 컨소시엄 형태의 단체이다. 초기 관심은 휴대용 하드웨어 장치에 집중되어서 휴대용 장치에 대한 규격인 페이즈 1의 버전 1.0을 제정하였으며, 현재는 본격적인 DRM 방식에 관한 페이즈 2에 대해 표준화를 진행중이다[4]. 이 규격에서는 DRM 기능이 내재된 음반을 안전하게 유통하도록 시스템을 규정하였다. MPEG-4와는 다르게 DRM 특성 자체가 규격에 포함되어 있다. SDMI 규격은 오디오 컨텐츠를 저장하고 연주하는 PDs(Portable Devices), PM(Portable Media)에 관해 성립되어 있다. 여기서 LCMs(Licensed Compliant Modules)은 어플리케이션과 PDs/PM 사이의 인터페이스 역할을 한다. SDMI 어플리케이션과 LCM에 한번 들어오거나, 또는 SDMI PD에 레코딩된 이후에는 모든 SD MI 컨텐츠가 컨텐츠 보호를 받도록 규정되어 있다. 그리고, 그 이후 저장, 전송 과정에서도 컨텐츠 보호를 유지해야 한다. SDMI 어플리케이션, PD, LCM은 각 컨텐츠를 제어하는 어떤 사용 규칙에 대해서도 적용될 수 있어야 한다. 기존 음반처럼 알려지지 않은 컨텐츠를 확인할 수도 있으며, 단 이 경우 복사는 불가능하다. 규격에는 어플리케이션과 장치의 인증 사항, SDMI에 속한 구성 요소들 -PM, 마이크로폰, 복사 과정, 스크리닝 방식- 간에 안전한 통신이 이루어지도록 필요한 사항을 기술하고 있다. 스크리닝은 불법 복사본을 감지하는 과정으로 이 방식에 대한 표준화 작업인 페이즈 2에 해당된다. 스크리닝 과정에서 불법 복제본으로 판정한 경우 SDMI 장치는 그것의 입력, 전송, 연주를 거부한다. 이러한 스크리닝은 디지털 워터마킹 기술을 기초로 한다. (그림 3)은 SDMI 구조로서 서버(호스트), PD, PM, LCM 인터페이스간의 상호 작용을 나타낸다.

현재, SDMI 컨소시엄에서는 휴대 전화와 같은 이동 단말기에 SDMI 개념과 PD 규격을 적용하는 작업을 진행중이다. 기본적으로 이것은 이동망 구조



(그림 4) 정보 은닉 기술의 분류

를 SDMI 서버-LCM-PM-PD 모델에 맞추는 것으로 휴대 장치 규격에서는 허가되지 않았던 내장형 마이크로폰을 허용하는 등 예외 규정에 대한 논의를 필요로 한다.

III. 워터마킹 기술

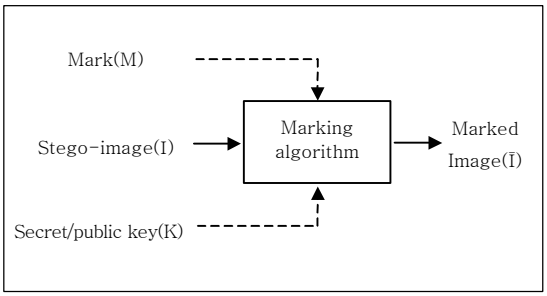
DRM 시스템의 요소 중 복사 제어 데이터 신원 확인과 역추적 부분을 위해서는 멀티미디어 데이터에 지워지지 않는 정보를 포함시킬 필요가 있다. 디지털 워터마크란 바로 이와 같이 멀티미디어 데이터에 첨부된 인지할 수 없는 정보를 의미한다. 워터마크가 가져야 할 기본 특성은 다음과 같다.

- 비인지성: 워터마크는 본 데이터에 인식할 만한 품질 손상을 일으켜서는 안 된다.
- 안전성: 정식 허가 받은 상태에서만 워터마크에 대한 접근이 가능해야 한다.
- 강인성: 여러 조작들, 특히 워터마크를 제거하려는 악의적인 공격 이후에도 남아 있어야 한다.

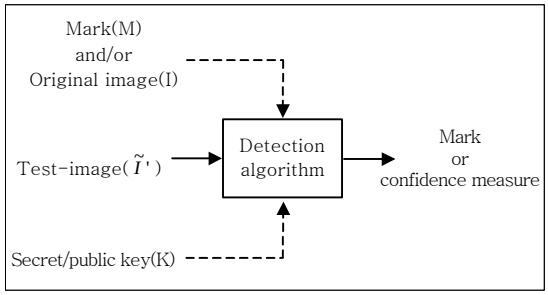
의심을 받지 않도록 하면서 비밀리에 정보 은닉을 하는 것은 고대로부터 내려오는 비화통신(steganography), 또는 정보 은닉 기술에서 유래한다. (그림 4)는 정보 은닉 기술의 여러 종류를 나타낸다[5].

대부분의 고대 시스템은 물리적으로 메시지를 은닉한 관점에서 기술적인 비화통신에 해당하고, 현대의 시스템은 언어적 비화통신 또는 저작권 마킹(copyright marking)에 해당한다. 비화통신은 은밀하게 이루어지고 있는 통신의 존재 자체를 숨기는 것으로 성공적인 공격이란 그 존재를 감지하는 것이 된다. 반면, 저작권 마킹은 정보를 제거하려는 공격에 대해 강인성을 갖춰야 하는 것이 둘 사이의 주요 차이점이다. 어플리케이션의 종류에 따라 마크의 성질을 다르게 할 수 있다. 예를 들어, 깨지기 쉬운 연성 워터마크(fragile watermark)는 데이터가 크게 변경될 경우 바로 파괴된다. 이것은 법정에서 데이터의 무결성을 증명하거나 그 외에 불법 복제나 유통의 목적으로 가해진 공격을 파악하는 지시 체계로 사용될 수 있다. 강성 워터마크(robust watermark)는 본 데이터를 파괴할 정도로 공격을 가하지 않고는 그것을 제거하거나 무용으로 할 수 없는 특성을 갖는다. 이 특성을 가지려면 데이터에서 지각될 수 있는 가장 중요한 부분에 마크를 삽입해야 한다. 강인한 워터마크 중 특별히 전자지문으로 이름 붙인 것은 일련번호처럼 동작하여 제3자에게 데이터를 불법적으로 제공한 사용자의 신원을 확인시켜 준다.

(그림 5)는 일반적인 삽입과정을 나타낸다[5]. 주어진 영상 I , 마크 M , 키 K (보통 난수 발생기



(그림 5) 일반적인 워터마크 삽입과정



(그림 6) 일반적인 워터마크 검파과정

의 시드)에 대해서 삽입과정은 다음의 매핑으로 정의된다: $I \times K \times M \rightarrow \tilde{I}$.

마찬가지로 검파과정은 (그림 6)과 같다[5]. 검파기의 출력은 추출된 워터마크 M 이 될 수도 있고, 어떤 확증을 위한 측정 값일 수도 있다. 검파과정의 입력으로 원본을 쓰는지에 따라 크게 프라이비트 시스템과 퍼블릭 시스템으로 나눌 수 있다.

- 프라이비트 마킹 시스템은 출력 특성에 따라 Type I과 Type II로 구분할 수 있다. Type I 시스템은 변형되었을 수도 있는 영상 $\tilde{I}'$ 에서 원 영상 I 를 이용하여 삽입한 마크 M 을 추출해 낸다. Type II 시스템은 입력으로 삽입한 워터마크도 필요로 하며, 이 때 출력결과는 "있다", "없다"로 나타난다. 즉, $\tilde{I}'$ 이 마크 M 을 포함하는가에 대해 답을 구하는 것으로 다음의 매핑과정으로 표현된다: $\tilde{I}' \times I \times K \times M \rightarrow \{0,1\}$. 이용하는 정보에 비해 추출 정보량이 적으므로 검파의 강인성을 기대할 수 있다. 세미프라이비트 마킹 시스템은 원 영상을 이용하지 않고 워터마크 유무를 검출한다: $\tilde{I}' \times K \times M \rightarrow \{0,1\}$. 이러한 프라이비트, 세미프라이비트 마킹 시스템은 주로 법정에서 소유권 증명을 위한 증거나 재생 허가를 필요로 하는 DVD 같은 어플리케이션에서 복제 제어용으로 사용된다.
- 퍼블릭 마킹은 블라인드 마킹으로도 불리며 원 영상이나 삽입된 마크를 쓰지 않고 원하는 결과를 검출하는 방식으로 여전히 도전 과제로 남아 있다. 매핑과정은 다음과 같다: $\tilde{I}' \times K \rightarrow M$. 퍼블릭 마킹 시스템은 응용분야가 훨씬 다양하지만, 삽입 알고리즘의 보안과 강인성 향상이 필수로 요구된다.

1. 다양한 정보 은닉 기술

가. 모호함을 이용한 보안

허가 받지 않은 사람은 정보 은닉에 사용된 시스템을 알 수 없다는 가정으로 비밀 통신을 하는 기술이다. 암호기술의 발전과정에서 알 수 있듯이 이 가정은 깨지기 쉽다. 왜냐하면 이 가정으로 형성된 시스템은 보안을 일종의 운에 맡기고 있는 셈이기 때문이다. 특히 현재 사용되는 대부분의 워터마크 알고리즘은 오디오나 비디오 신호 데이터의 최하위 비트에 데이터를 '은닉'하고 있는데, 이것은 적이 은닉 데이터를 제거하고자 할 때 가장 먼저 확인하는 곳이다.

나. 위장

시각을 변경하면 다른 그림이 되거나 위험한 정치적 발언을 교묘하게 숨기는 데 사용된 그림 등이 15~17세기에 사용된 비화통신의 위장 기술이다. 최근에는 특별한 잉크, 또는 형광염색이나 DNA와 같이 독특한 구조를 갖는 물질로 메시지를 작성하여 은닉하는 기술도 생겨났다. 이것은 이 물질들이 어떤 시약이나 특정 주파수의 레이저 빛에 대해 고유한 반응을 나타내는 것을 이용한 것이다[6]. 디지털에서 위장 기술에 대응하는 것은 소스 코딩과 같은 마스킹 알고리즘이라고 할 수 있을 것이다[7]-

[11]. 이것은 인간의 지각 시스템에 기초하는 것으로 오디오 마스킹을 예로 들면, 가까운 주파수 영역에서 두 개의 톤이 동시에 발생했을 때 소리가 큰 톤이 작은 것을 마스킹한다. 시간영역에서도 마찬가지로 큰 음원은 그 전후의 작은 음원을 마스킹하는 특성을 가지며 이러한 마스킹 효과는 MPEG와 같은 압축 표준에 이용되고 있다. 워터마크 시스템에서는 삽입할 데이터의 모양을 다듬기 위해 마스킹 효과를 이용한다. 워터마크가 압축 등의 신호처리에서 살아남으려면 지각적으로 인식할 수 있는 중요한 부분에 삽입되어야 하는데, 이 때 마스킹 곡선에 최대한 근접할 때까지 워터마크의 크기를 증폭시켜서 강인성을 키울 수 있다.

다. 정보 삽입 위치 은닉

고대 중국에서 종이 마스크를 이용하여 비밀 통신을 한 것이 이 기술의 한 예이다. 송신자는 종이 위에 종이 마스크를 놓고 마스크의 구멍 뚫린 부분에 메시지를 적는다. 마스크를 제거한 다음 메시지가 드러나지 않도록 작문한다. 수신자는 받은 종이 위에 마스크를 놓고 읽으면 된다. 현재의 저작권 마킹은 오디오, 정지영상, 비디오 등 멀티미디어 개체의 디지털 형태에 대한 것이 주요 관심사인데 앞서 언급했듯 많은 저자들이 최하위 비트에 데이터를 삽입하는 것을 제안하고 있다[12],[13]. 이 때 데이터를 삽입하는 픽셀이나 음원 샘플을 무작위로 선택한다면 보안이 좀 더 강화될 수 있을 것이다[14],[15]. 이 방식에서는 근사 무작위 수열 발생기의 시드가 시스템의 보안키로 설정된다. 구현할 때에는 좀 더 세심한 주의가 필요하다. 예를 들어 영상에서 단조로운 색이 넓게 퍼진 부분이나 날카로운 모서리 부분의 픽셀을 변화시키는 것은 피해야 한다. 즉, 흑백의 경우에는 명암의 분산이 지나치게 크거나 작은 픽셀을 제외시키고 선택해야 한다. 또, 간단한 디지털 필터링만으로도 디지털 개체의 최하위 비트를 다량으로 변화시킬 수 있으므로 이러한 필터링에 대한 강인성을 고려해야 한다.

라. 은닉 정보의 분산

정보를 분산시키는 확실한 방법으로 삽입한 데이터 채널에 의도적으로 잡음을 첨가하는 필터 처리와 남는 밴드대역을 활용하여 적절한 코딩을 하는 것을 생각해 볼 수 있다. 가장 단순한 방법으로는 반복코드가 있다. 즉, 한 비트를 충분한 시간 동안 삽입하여 필터 통과 후에도 살아 남게 하는 것인데 코딩 이론 관점에서는 비효율적이지만, 간단하고 어떤 어플리케이션에 대해서는 강인할 수 있다. 다른 방법으로 패치워크라고 불리는 방식은 픽셀의 밝기에 대한 확률을 이용한다[16]. 예를 들어 난수 발생기로 n 쌍의 픽셀을 선택하여 광도 명암을 미세하게 증가시키거나 감소시킨다. 그러면 전체 영상의 평균 광도를 변화시키지 않고, 이 세트들의 명암만 증가시키게 된다. 그러나 이 경우 1비트 정보만 삽입할 수 있으며 더 많은 정보를 삽입하려면 영상을 조각으로 나눈 후 각 조각에 정보를 삽입해야 한다. 이 방법은 대역확산 변조방식의 기초가 되었다. Tirkel의 디지털 워터마크 이래로 대역확산 기술을 응용한 워터마크의 연구가 많이 이루어졌다[10],[17]-[20]. 이 방법은 상대적으로 좁은 대역의 워터마크를 넓은 대역의 커버 미디어에 대응시키는 데 큰 장점을 갖는다.

Cox는 영상의 이산 코사인 변환(DCT)에서 지각적으로 중요한 n 개의 주파수 성분 $V = \{v_i\}_{i=1}^{n}$ 에 워터마크 데이터를 삽입하는 방식을 제안하였다[21]. 이 방식은 프라이비트 마킹 시스템의 Type II에 해당하는데 먼저 정규 분포를 갖는 실수열 $W = \{w_i\}_{i=1}^{n}$ 를 워터마크 데이터로 생성한 뒤, 다음 식을 이용해서 삽입한다: $\tilde{v}_i = v_i(1+\alpha w_i)$. I , $\tilde{I}$ 를 각각 원 영상과 워터마크가 삽입된 영상이라고 할 때, I 에서 주 성분을 추출함으로써 워터마크의 존재를 확인할 수 있다. $\tilde{I}$ 의 같은 색인에 해당하는 성분에서 삽입과정을 역으로 수행하여 변형되었을지도 모르는 워터마크 W' 을 추출해낸다. $W \cdot W' / \sqrt{W' \cdot W'}$ 의 값이 일정 문턱 값 이상이면 워터마크가 있다고 판단한다. 이 방식은 리스케일링, JPEG 압축, 떨림, 클리핑, 프린팅/스캐닝, 콜루전 공격 등

에 대해 매우 강인하지만, 몇 가지 단점이 있다. 가장 심각한 문제는 워터마크의 존재를 확인하기 위해 원 영상을 필요로 하는 것이다. 두번째는 패치워크와 마찬가지로 삽입할 수 있는 정보량이 작다는 것이다. 따라서, 전자지문으로는 부적합하며, 영상을 쪼개어 삽입한다면 정보량은 늘일 수 있지만 강인성이 떨어진다.

삽입하는 정보를 효율적으로 분산시키기 위해서 미디어 데이터를 다른 영역으로 변환시키고, 그 변환 영역에서 정보를 은닉하는 방식에 대한 연구가 증가하고 있다. 이 방식은 압축과 일반 필터처리, 잡음에 강인한데 실제로 어떤 특정 변환을 사용한 워터마크는 그 변환에 기초한 압축 알고리즘에 강인한 것을 관측할 수 있다. 또 압축된 개체를 직접 다루기도 한다[20]. gif 파일에서 선택된 픽셀의 색깔을 그 팔레트의 이웃색깔로 바꾸는 것이나 MP3의 압축과정에서 삽입하는 것이 그 예이다[22],[23]. 그러나 대부분의 방식은 커버 개체의 DCT[7],[21],[24]-[27], 웨이브렛[7],[28], 이산 푸리의 변환과 같이 개체 자체의 변환영역에 직접 적용한다[10],[29].

오디오 데이터 변환의 새로운 방식으로 반향 삽입 방법이 있다. 이것은 인간의 청각시스템이 수 밀리 초의 짧은 반향은 인지할 수 없다는 사실에 기초한 것으로 1과 0을 나타내는 두 가지 종류의 반향을 삽입하여 데이터를 은닉하는 것이다[30]. 이 비트들은 임의의 길이만큼의 간격을 두고 코딩되며, 켑스트럼 변환을 이용하여 반향신호를 처리한다[31].

2. 워터마킹 기술의 몇 가지 한계

디지털 워터마크와 전자지문의 다양한 기술들이 제안되면서 각 방식이 저마다 '강인성'을 주장해왔다. 그러나 불행하게도 시스템마다 강인성 기준과 증명에 사용된 영상들에 상당한 편차가 있고, 최근 워터마크에 대한 공격들이 보여주듯 이제까지 사용된 강인성 기준들도 종종 부적합한 것으로 드러났다[32]-[36]. 지금까지 대부분의 워터마크 시스템에서 JPEG 압축, 정규 잡음 첨가, 저대역 필터링, 리스케일링, 커팅 등을 다루고 있으나 회전과 같은 특별한 왜곡은 거의 무시되었다[29],[37]. 어떤 경우에는 간단히 "몇 개의 표준 영상에 대해서 일반적인 신호처리 알고리즘과 기하학적인 왜곡의 강인함"으로 표현되기도 한다. 이처럼 아직까지 명확하게 정해진 기준이 없어서 디지털 워터마크의 강인성에 대한 공정한 기준의 필요성이 대두되고 있다[38].

디지털 워터마크에 대한 공격은 크게 다음의 세 종류로 분류된다[39]. 먼저 강인성 공격은 디지털 워터마크를 제거하거나 사라지게 할 목적으로 신호처리를 한다. 존재 공격은 모자이크 공격처럼 검파기가 워터마크를 찾아내지 못하도록 컨텐츠를 변형시키는 것이고, 마지막으로 해석 공격은 소유권 주장이 무효화되도록 특별한 상황을 형성하는 것이다. 각 공격들을 이렇게 구분하는 것이 언제나 명확한 것은 아니어서 스터마크(StirMark) 공격은 워터마크를 사라지게 하거나 검출하지 못하도록 컨텐츠를 변형시키는 두 가지를 다 포함하고 있다.

가. 기본 공격(Basic Attack)

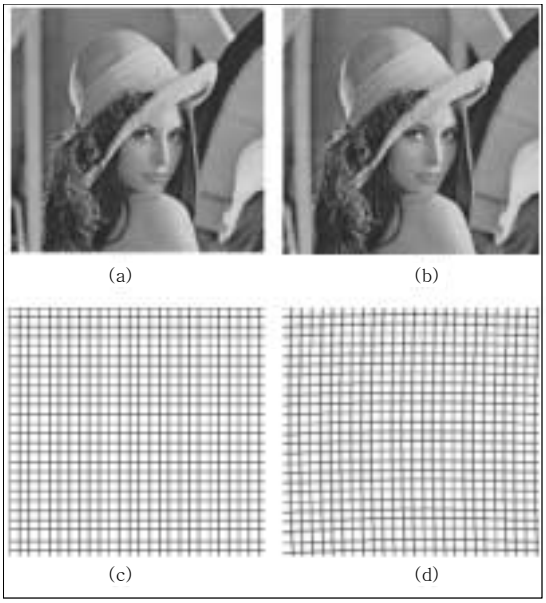
대역 확산 신호는 크기 변형이나 잡음 첨가 등에는 매우 강인하지만, 타이밍 오류에는 살아 남지 못한다[34]. 칩 신호의 동기는 매우 중요하며, 단순한 시스템에서는 동기 작업에 실패하기 쉽다. Hamdy는 피치를 변화시키지 않고, 음악작품의 길이를 늘이거나 줄이는 방법을 제시하였다[40]. 이것은 방송 시간을 맞추기 위해 미세한 조정이 필요할 경우 응용 가능할 뿐 아니라 소리 조작에 필요한 공격을 쉽게 만든다.

나. 강인성 공격(Robustness Attack)

1) 스터마크

개발된 워터마크 시스템의 대부분이 기본 조작에는 강인하다. 즉 회전, 리샘플링, 크기 조절, 손실 압축 등 표준 도구로 쉽게 할 수 있는 조작들에는 살아남지만, 그것들의 조합과 무작위 기하학적 왜곡에는 버티지 못하였다. 이러한 결과들로부터 영상 워터마

크 알고리즘의 기본적인 테스트 도구로서 스터마크가 개발되어 사용중이다[34]. 스터마크는 임의의 미세한 양으로 스트레치, 쉬어링, 벤트, 회전 등의 기하학적인 왜곡을 가한다. 그리고, 각 픽셀에 임의로 미세하게 저대역 편향을 가하는데 편향 정도는 영상의 중앙부에 가장 크게 나타난다. 고대역 부분은 $\lambda \sin(w_x x)\sin(w_y y) + n(x, y)$ 식의 값으로 대체하는데, 이 때 $n(x, y)$ 는 난수이다. 마지막으로 변환 함수를 적용하여 전 샘플에 원만한 분포를 갖는 작은 양의 오류를 첨가한다. 이것은 비선형 아날로그/디지털 변환기의 전형적인 결함 형태를 에뮬레이션한 것이다. 리샘플링은 정방형의 B 스플라인 근사 알고리즘을 이용한다[41]. 이 변형의 예는 (그림 7)에 나타내었다[5]. 이 외에 스터마크는 영상 워터마크의 성능평가로 쓰이는 기본 공격을 연속 수행할 수도 있다.



(그림 7) 스터마크로 영상에 변형을 가했을 경우, (a), (b)는 "Lena" 영상의 변형 전, 변형 후, (c), (d)는 비교를 위한 격자영상의 변형 전, 변형 후

2) 반향 삽입에 대한 공격

앞서 기술한 대로 반향 삽입 코딩은 0과 1에 해당하는 두 개의 다른 반향신호 즉 지연시간 τ , 상대크기 α 가 구별되는 신호를 커버 오디오 신호에 삽입하는 방식이다[30]. 지연시간은 0.5에서 2밀리초 사이이며, 상대 크기는 대략 0.8 부근이다. 검출을 위해서 먼저, 초기 지연시간을 켑스트럼의 자기 상관 값을 이용해서 찾는다. 그런데 공격을 위해서도 같은 기술이 쓰일 수 있다. 반향 삽입에 대한 확실한 공격방법은 반향을 찾아서 그것을 제거하는 것이다. 문제는 본 개체와 반향의 매개 변수 등을 모르는 상태에서 반향을 찾는 것인데, 켑스트럼 분석을 이용하여 반향 지연시간 τ 를 찾을 수 있다[31]. 주어진 신호 $y(t)$ 가 단순히 한 개의 반향 신호를 포함한다면, $y(t) = x(t) + \alpha x(t-\tau)$ 이다. Φ_{xx} 를 x 의 전력 스펙트럼이라고 하면, $\Phi_{yy}(f) = \Phi_{xx}(f)(1 + 2\alpha\cos(2\pi f\tau) + \alpha^2)$ 이며 로그를 취하면 다음과 같은 근사식을 얻을 수 있다: $\log \Phi_{yy}(f) \approx \log \Phi_{xx}(f) + 2\alpha\cos(2\pi f\tau)$. 이것의 전력 스펙트럼을 구하면 τ 의 함수로 나타나고, 자기 공분산을 취하게 되면 τ 에서 피크가 두드러지게 나타난다. 이것은 약간 변형된 형태의 켑스트럼으로서 다음 식으로 정의할 수 있다. $C \circ \Phi \circ \ln \circ \Phi$, 여기서 C 는 자기 공분산 함수이고, Φ 는 전력 스펙트럼, $\circ$ 는 합성 연산자이다: $(C(x) = E((x - \bar{x})(x - \bar{x})^*))$.

3) 다른 일반적인 공격

Langelaar는 대역 확산을 이용한 백색 워터마크에 대한 공격을 제안하였다[35]. 이 방법은 원 영상에 대해 모델링을 하여 워터마크가 삽입된 영상 $\tilde{I} = I + W$ 로부터 원 영상에 대한 추정 값 $\hat{I}$, 워터마크 추정 값 $\hat{W}$ 를 분리하는 것이다. 이 때 추정 값들은 $\rho(\hat{I}, W) \approx 0$ 의 관계를 만족시킨다. 이 경우 워터마크의 저대역 성분은 정확한 추정이 어려우므로 상관 값 ρ 에 대해 저대역 성분은 양수로, 고대역 성분은 음수로 영향을 끼친다. 따라서 추정된 워터마크에 대해 적절한 증폭 계수를 선택하는 작업이 필요하다. 어떤 경우에는 영상의 특징상 악의적인 공격을 돕는 수도 있다. 만화 영상과 같이 색깔 구분이 뚜렷하고 그 숫자가 적은 영상은 색 히스토그램

에서 날카로운 피크를 드러낸다. 이러한 영상은 몇몇 워터마크 알고리즘으로 쪼개지는데 Maes가 제안한 짝 피크 공격은 이 특성을 이용하여 마크를 추출하고 제거한다[33]. 흑백 영상에 대역 확산 디지털 워터마크를 단순하게 삽입하는 방식은 영상의 각 픽셀을 임의로 고정 값 d 만큼 증가시키거나 감소시키는 것이다. 따라서 각 픽셀 값은 증가되거나 감소되었을 가능성이 50%인 셈이다. n_k 를 흑백 명암 값이 k 인 픽셀의 수라고 하자. k_0 의 d 번째 주변 값을 갖는 픽셀이 없으면, $n_{k_0-d} = n_{k_0+d} = 0$ 이 된다. 따라서 워터마킹 이후에 다음과 같은 기대 값을 구할 수 있다. $\tilde{n}_{k_0-d} = \tilde{n}_{k_0+d} = n_{k_0}/2$, $\tilde{n}_{k_0} = 0$. 그러므로 다른 세트에 대해서도 비슷한 방정식을 적용하면 원래 히스토그램의 분포를 복구하고 삽입한 워터마크의 값을 알아내는 것이 가능하게 된다.

다. 존재 공격(The Mosaic Attack)

모자이크 공격은 네트워크에서 영상을 다운로드 받아서 고객 워터마크를 체크하는 웹 크롤러의 활성화로 출현하게 되었다. 이 공격은 존재 공격의 일종으로 영상을 다수의 작은 영상들로 쪼갠 다음에 웹 페이지에서 차례로 삽입한다. 보통의 웹 브라우저는 부분 영상들을 병렬로 배치하여 하나의 영상들로 합쳐주므로, 결과적으로는 원본과 같게 된다. 이 방식은 웹에서 매우 강력한 공격이 될 수 있다. 왜냐하면 모든 마킹 시스템은 영상의 크기가 어느 정도 되어야 제대로 동작할 수 있기 때문이다(하나의 픽셀에 의미있는 마크를 삽입할 수 없다). 그러므로 적절하게 영상을 조각 낼 경우 워터마크 검출기는 혼란을 일으킬 것이다. 그러나 워터마크 시스템에서 요구하는 영상의 최소 크기를 상당히 작게 한다면 이 공격은 막을 수 있다[34]. 이 공격 외에도 "크롤러"에는 여전히 다른 문제들이 남아 있다. 자바 애플릿 같은 이동 코드는 브라우저 내에 영상을 출력하기 위해 사용되는데, 애플릿은 실시간으로 영상을 다시 정리할 수 있다. 이러한 기술에 대응하려면 전체 페이지에 대해 영상을 검증하고, 마크를 확인하는 과정을 거쳐야 한다.

라. 해석 공격(Interpretation Attack)

이제까지 설명한 공격 방법들은 기술적인 처리로 워터마크를 직접 제거하려는 시도였고, 보통 강인성이라고 할 때는 오직 이러한 신호처리 조작에 대한 저항성을 의미한다. 그러나 Carver는 프로토콜 레벨에서의 공격을 예로 들면서 이 정의만으로 부족함을 보였다[42]. 이 공격의 기본 개념은 두 개의 워터마크가 있을 때 어느 것이 먼저 삽입된 것인지를 검출할 수 있는 방법이 뚜렷하지 않다는 데 기초한다. 문서 d 의 소유자가 워터마크 w 를 삽입하여 $d+w$ 버전을 출판했을 때 해적이 자기 워터마크 w' 에 대하여 원본이 $d+w-w'$ 라고 주장할 경우, 워터마크 버전에서 원본을 빼는 방법으로는 소유권을 증명할 수 없다. 이러한 해석 공격에 대한 대안은 워터마크나 전자지문 방식을 단독으로 쓰지 않고, 출판 시간기록이나 인증 등의 과정을 포함하는 큰 시스템의 부분으로 사용하는 것이다.

마. 구현 관점(Implementation Consideration)

삽입과 추출의 알고리즘, 프로토콜 외에 고려해야 할 부분이 있다. 이전에 구현된 많은 암호 시스템에서 대부분의 실제 공격은 우연히 발견된 구현 상의 버그를 이용하였으며 암호분석은 거의 이용되지 않았다[43]. 워터마크 시스템에서의 공격도 마찬가지라고 예상할 수 있는데 실제로 인터넷 상에서 일어난 첫번째 공격도 알고리즘보다는 구현의 약점을 이용한 것이었다(스터마크로 신호처리를 하면 제거될 수 있는 약한 마크였다). 공격자는 먼저 디버거를 이용하여 소프트웨어를 분해한 후, 패스워드-확인 과정을 무효화하였다.

Ⅳ. 결론 및 향후 연구방향

본 고에서는 디지털 저작권 관리(DRM)를 위해 필요한 요소 기술과 DRM의 기술 개발 및 표준화 현황을 기술하였고, 최근 DRM의 세부 중요 기술로 부각

되고 있는 워터마크 기술의 특성을 살펴 보았다. 네트워크와 미디어의 발달로 멀티미디어 데이터의 불법 유통이 급속히 확산되고 있기 때문에, 향후 E-, M-, T-상거래의 안정적인 발전을 위해서는 디지털 데이터의 저작권 관리와 보호가 반드시 필요하게 되었다.

많은 단체에서 저작권 관리에 대한 알고리즘을 개발하고, 표준화 작업을 진행시키고 있는데 특히 복제 제어와 전자지문에 관계된 워터마크는 알고리즘의 잠재적 개발 가능성 때문에 활발한 연구가 진행되고 있다.

그러나, 현재의 워터마크 기술은 아직까지 암호화 기술만큼 안전하지 않으며, 대부분 강인성과 정보량, 품질에 대해 트레이드오프 상태에 있어서 전체 저작권 관리 기술에 직접 적용하기에는 아직 부족한 기술로 간주되고 있다. 따라서 워터마크는 단독적 기술이 아니라 시스템의 한 구성 요소로 고려되어야 할 것이며, 향상된 알고리즘의 개발을 위해서는 공정한 성능평가 지침이 선행될 필요가 있다.

워터마크를 비롯한 저작권 관리와 보호에 관한 기술들은 시스템의 요구사항에 따라 적용되는 기술의 종류와 강인성이 달라지게 된다. 따라서 저작권 관리 시스템 개발을 위해서는 먼저 전체 시스템의 요구사항을 분명하게 정의하고, 필요한 기술의 최적화를 위한 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] M. Miller, I.J. Cox, and J. Bloom, "Watermarking in the Real World: an Application to DVD," *Proc. Workshop Multimedia and Security at ACM Multimedia 98*, Bristol, U.K., Sep. 1998.

[2] F. Hartung and F. Ramme, "Digital Rights Management and Watermarking of Multimedia Content for M-commerce Applications," *IEEE Commun. Magazine*, Nov. 2000, pp. 78 - 84.

[3] J. Lacy, N. Rump, and P. Kudumakis, "MPEG-4 Intellectual Property Management & Protection (IPMP) Overview and Applications," *MPEG doc.* ISO/IECJTC1/SC29/WG11/N2614, Dec. 1998.

[4] SDMI, "SDMI Portable Device Specification, part 1, version 1.0," *SDMI doc.* Pdwg99070802, July 1999, http://www.sdmi.ofg/.

[5] F. Petitcolas, R. Anderson, and M. Khun, "Information Hiding – a Survey," *Proc. IEEE*, July 1999, pp. 1062 – 1078.

[6] J.C. Murphy, D. Dubbel, and R. Benson, "Technology Approaches to Currency Security," *in Optical Security and Counterfeit Deterrence Techniques II*, Vol. 3,314, R.L. van Renesse, Eds. San Jose, CA: IS&T and SPIE, 1998, pp. 21 - 28.

[7] C.I. Podilchunk and W. Zeng, "Digital Image Watermarking Using Visual Models," *in Human vision and Electronic Imaging II*, Vol. 3,016, B.E. Rogowitz and T.N. Papps, Eds. San Jose, CA: IS&T and SPIE, 1997, pp. 100 - 111.

[8] M.D. Swanson, B. Zu, and A.H. Tewfik, "Robust Data Hiding for Images," *in Proc. IEEE 7th Digital Signal Processing Workshop 96*, Loen, Norway, Sep. 1996, pp. 37 - 40.

[9] J.F. Delaigle, C. De Vleeschouwer, and B. Macq, "Watermarking Algorithm Based on a Human Visual Model," *Signal Processing*, May 1998, pp. 319 - 335.

[10] L. Boney, A.H. Tewfik, and K.N. Hamdy, "Digital Watermarks for Audio Signals," *in Proc. IEEE Int. Conf. Multimedia Computing and Systems*, Hiroshima, Japan, Hune 1996, pp. 473 - 480.

[11] F. Goffin, J. – F. Delaigle, C.D. Vleeschouwer, B. Macq, and J. – J. Quisquater, "A Low Cost Perceptive Digital Picture Watermarking Method," *in Storage and Retrieval for Image and Video Database V*, Vol. 3,022, I.K. Sethin and R.C. Jain, Eds. San Jose, CA: IS&T and SPIE, 1997, pp. 264 - 277.

[12] R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne, "A Digital Watermark," *in Proc. IEEE Int. Conf. Images Processing*, Vol. 2, Austin, TX, 1994, pp. 86 - 90.

[13] R.B. Wolfang and E.J. Delp, "A Watermark for Digital Images," *in Proc. IEEE Int. Conf. Images Processing*, Lausanne, Switzerland, Sep. 1996, pp. 219 - 222.

[14] S. Walton, "Image Authentication for a Slippery New Age," *Dr. dobb's J. Software Tools*, Vol. 20, No. 4, Apr. 1995, pp. 18 - 26.

[15] K. Matsui and K. Tanaka, "Video-steganography:

How to Secretly Embed a Signature in a Picture," *J. Interactive Multimedia Association Intellectual Property Project*, Vol. 1. No. 1, Jan. 1994, pp. 187 - 205.

[16] W. Bender, D. Gruhl, N. Mrimoto, and A. Lu, "Techniques for Data Hiding," *IBM Syst. J.*, Vol. 35, 1996, pp. 313 - 336.

[17] A.Z. Tirkel, G.A. Rankin, R.M. van Schyndel, W.J. Ho, N.R.A. Mee, and C.F. Osborne, "Electronic Watemark," *in Digital Image Computing, Tech. And App. 93*, Macquarie University, Sydney, Australia, 1993, pp. 666 - 673.

[18] J.R. Smith and B.O. Comiskey, "Modulation and Information Hiding in Images," *in Information Hidng: 1st Int. Workshop(Lecture Notes in Computer Science)*, Vol. 1,174, R.G. Anderson, Eds. Berlin, Germany: Springer Verlag, 1996, pp. 207 - 226.

[19] I.J. Cox, J. Kilian, T. Leighton, and T. Shmoon, "Secure Spread Spectrum Watermarking for Images Audio, and Video," *in Proc. IEEE Int. Conf. Image Processing 96*, Lausanne, Switzerland, Sep. 1996, pp. 243 - 246.

[20] F. Harung and B. Girod, "Watermarking of MPEG-2 Encoded Video without Decoding and Re-encoding," *in Multimedia Computing and Networking 1997*, Vol. 3,020, M. Freeman, P. Jardetzky, and H.M. Vin, Eds. San Jose, CA: IS&T and SPIE, 1997, pp. 264 - 273.

[21] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A Secure, Robust Watermark for Multimedia," *in 1st Int. Workshop(Lecture Notes in Computer Science)*, Vol. 1,174, R.G. Anderson, Eds. Berlin, Germany: Springer Verlag, 1996, pp. 183 - 206.

[22] G. Jagpal, "Steganography in Digital Images," Ph.D Dissertation, Selwyn College, Cambridge Univ., Cambridge, U.K., May 1995.

[23] F.A.P. Petitcolas, MP3Stego. [Online] available, http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego/.

[24] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-domain System for Robust Image Watermarking," *Signal Processing*, Vol. 66, May 1998, pp. 357 - 372.

[25] E. Koch and J. Zhao, "Toward Robust and Hidden Image Copyright Labeling," *in Proc. IEEE Workshop Nonlinear Signal and Image Processing*, Neos Marmars, Greece, June, 1995, pp. 452 - 455.

[26] J.J.K. O'Ruanaidh, W.J. Dowling, and F.M. Boland, "Watermarking Digital Images for Copyright Protection," *Proc. Inst, Elect. Eng. Bision, Signal and Image Processing*, Vol. 143, Aug. 1996, pp. 250 - 256.

[27] M.D. Swanson, B. Zhu, and A.H. Tewfik, "Transparent Robust Image Watermarking," *in Proc. IEEE Int. Conf. Image Processing*, Vol. III, 1996, pp. 211 - 214.

[28] D. Kundur and D. Hatzinakos, "A Robust Digital Image Watermarking Method Using Wavelet-based Fusion," *in Proc. IEEE Int. Conf. Image Processing*, Santa Barbara, CA, Oct. 1997, pp. 544 - 547.

[29] J.J.K. O'Ruanaidh and T. Pun, "Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking," *Signal Processing*, Vol. 66, May 1998, pp. 303 - 317.

[30] D. Gruhl, W. Bender, and A. Lu, "Echo Hiding," *in-Information hiding: 1st Int. Workshop(Lecture Notes in Computer Science*), Vol. 1,174, R.J. Anderson, Eds. Berlin, Germany: Springer-Verlag, 1996, pp. 293 - 315.

[31] B.P. Bogert, M.J.R. Healy, and J.W. Tukey, "The Quefrency Analysis of Time Series for Echoes: Cepstrum, Pseudo-autocavariance, Crosscepstrum and Saphe Cracking," *in Symp. Time Sereies Analysis*, M. Rosenblatt, Eds. New York: Wiley, 1963, pp. 209 - 243.

[32] J. – P.M.G. Linnartz and M. van Digk, "Analysis of the Sensitigity Attack Against Electronic Watermarks in Images," *in Information Hiding: 2nd Int. Workshop(Lecture Notes in Computer Science)*, Vol. 1,525, D. Aucsmith, Eds. Berlin, Germany: Springer-Verlag, 1998, pp. 258 - 272.

[33] M. Maes, "Twin Pears: The Histogram Attack on Fixed Depth Image Watermarks," *in Information Hiding: 2nd Int. Workshop(Lecture Notes in Computer Science)*, Vol. 1,525, D. Aucsmith, Eds. Berlin, Germany: Springer-Verlag, 1998, pp. 290 - 305.

[34] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Attacks on Copyright Marking Systems," *in Information Hiding: 2nd Int. Workshop(Lecture*

Notes in Computer Science), Vol. 1,525, D. Aucsmith, Eds. Berlin, Germany: Springer-Verlag, 1998, pp. 218 - 238.

[35] G.C. Langelaar, R.L. Lagendijk, and J. Biemond, "Removing Spatial Spread Spectrum Watermarks by Nonlinear Filtering," *in 9th European Signal Processing Conference 98*, Rhodes, Greece, Sep. 1998, pp. 2281 – 2284.

[36] R. Barnett and D.E. Pearson, "Frequency Mode LR Attack Operator for Digitally Watermarked Images," *Electron Lett.*, Vol. 34, Sep. 1998, pp. 1837 – 1839.

[37] M. Kutter, "Watermarking Resisting to Translation, Rotation, and Scaling," *in Proc. SPIE Multimedia Systems and Applications*, Vol. 3,528, Boston, MA, Nov. 1998, pp. 423 - 431.

[38] M. Kutter and F.A.P. Petitcolas, "A Fair Benchmark for Image Watermarking Systems," in 11th Int. Symp. Electronic Imaging, Vol. 3,657, San Jose, CA: IS&T and SPIE, Jan. 1999.

[39] S. Craver, B. - L. Yeo, and M. Yeung, "Technical Trials and Legal Trivulations," *Commun. ACM*, Vol. 41, July 1998, pp. 44 - 54.

[40] K.N. Hamdy, A.H. Tewfik, T. Chen, and S. Takagi, "Time Scale Modification of Audio Signals with Combined Harmonic and Wavelet Representations," *in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing 97*, Vol. 1, Munich, Germany, pp. 439 - 442.

[41] N.A. Dodgson, "Quadratic Interpolation for Image Resampling," *IEEE Trans. Image Precessing*, Vol. 6, Sep. 1997, pp. 1322 - 1326.

[42] S. Craver, N. Memon, B. - L. Yeo, and M.M. Yeung, "Can Invisible Watermark Resolve Rightful Ownerships?," *in Storage and Retrieval for Image and video Database V*, Vol. 3,022, I.K. Sethin and dR. C. Jain, Eds. San Jose, CA: IS&T and SPIE, 1997, pp. 310 - 321.

[43] R.J. Anderson, "Why Cryptosystems Fail," *Commun. ACM*, Vol. 37, Bov. 1994, pp. 32 - 40.