워터마킹 기술 중심의 저작권 보호 기술

(Copyright protection using watermarking)

이영아 · 하재호

1. 서 론

1.1 개발개요

본 기술개발은 인터넷망을 통한 멀티미디어 컨텐츠(영상, 정지영상, 동영상, 오디오, 문서 등)의 유통에 따른 지적소유권, 저작권을 보호하기 위한 워터마킹 시스템 구축에 목적을 둔다.

개인용 컴퓨터의 보급 확대와 네트워크의 급속한 성장으로 인해 정지영상, 문서, 동영상, 음악 데이터 등의 멀티미디어 보급이 급격히 증가하고 있다. 이러한 보급에 힘입어 누구나 손쉽게 디지털 컨텐츠를 얻을 수 있게 되었고, 불법적인 복제나 보급 또한 증가하고 있다. 이에 불법적인 데이터 복제를 막고, 데이터 보급자의 저작권과 소유권 보호의 필요성이 대두되었다.

1.2 저작권 보호의 방법론

대부분의 워터마킹 기술들은 대략적으로 두 가지로 분류할 수 있다. 먼저, 어떤 변환에 의한 계수의 변화이거나 직접적인 픽셀 값의 변환이다. 이러한 기술들은, 인간 시각기관의 특성을 고려하여 육안으로는 거의 식별할 수 없는 정도로 데이터 값을 왜곡하는 방법으로 워터마킹을 하는 경우이다. 이러한 변환에 기반한 기술들은 대부분 DCT, DFT, Wavelet 등의 변환을 사용하며, 일반적으로 키 값에 의한 변환이다.

워터마크 패턴은 자체 주파수 영역에서의 에너지가 저주파나 고주파에 의존하는 기술이다. 노이즈와 같은 워터마크를 스프레드 스펙트럼 방법으로 공간적으로나 주파수 영역상에서 생성하도록 하여 통계적인 직교성으로 원 이미지에 삽입하고 단순한 점 형태로 워터마크 된 이미지나 스펙트럼의 일부분으로 추출을 한다.

저주파 영역의 워터마킹 방법은 저주파영역에 이미지데이터의 대부분이 몰려있는 것을 이용하여 여기에 워터마크신호를 겹치게 하는 것을 기본적인 접근방법으로 한다.

1.2.1 공간영역에 의한 워터마킹

워터마크를 삽입하는 방법이나 응용기술에 따라 데이터를 공간적 관점에서 삽입하는 방법(Spatial Method), 주파수 영역에서 삽입하는 방법(Frequency Domain Method)으로 나눌 수 있다. 공간적인 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 사용하는 방법이다. 이 방법은 워터마크의 삽입은 쉽지만, 손실압축(JPEG)이나

*중소기업중앙회 여성특별위원회 위원
**(주)컨텐츠코리아 기업부설연구소 소장

필터링과 같은 이미지 처리에 약하다는 단점이 있다.

1.2.2 주파수 영역에서의 워터마킹

최근에 가장 많이 이용되는 것이 데이터를 주파수 공간 변환(frequency domain transforms)으로 워터마킹 하는 기술이다. 이 방법은 공간적 분석을 통한 워터마킹보다 여러 가지 장점을 가지고 있으며, 그림 1은 주파수 영역에서의 워터마킹의 일반적인 절차를 보여 준다. 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), 고속 푸리에 변환(FFT) 그리고 웨이브렛 변환(Wavelet Transform) 등을 이용한다. 이 방법은 삽입하려는 워터마크 계수(데이터)들이 원 데이터의 전 영역에 분포하게 되며 한번 삽입된 워터마크는 삭제가 어려운 장점이 있다.

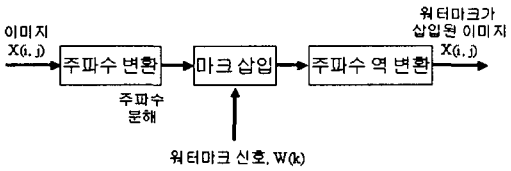

그림 1. 주파수 영역에서의 워터마킹 알고리즘

1.2.3 비가시적인 워터마킹(Zhao & Koch's Algorithm)

Zhao와 Koch의 논문에서 제안한 방법으로 이 방법은 이산 코사인 변환(Discrete Cosine Transform)계수에 비트 스트림을 삽입하는 방법으로 JPEG압축방법과 같이 이미지를 8×8블록으로 나눈 다음 이 블록에 대하여 이산 코사인 변환 계수를 계산한다. 이 계수를 이미지의 질을 결정하는 Q-factor와 JPEG의 표준 양자화 행렬(standard quantization matrix)로 양자화를 하고 양자화 된 3개의 블록을 비교하는 데, 세 번째 블록의 계수가 다른 두 개의 블록의 계수보다 작을 경우에는 블록을 '1'로 부호화 한다.

그러므로 주파수에 마스킹하는 것과 같은 현상을 얻은 이 방법은 각각의 블록이 DCT 변환되며, 주파수 마스킹 모델을 이용하여 DCT 주파수 계수각각에 허용 가능한 최대치 변화를 계산하여 워터마크를 구조화한다. 그러므로 다른 제 3자가 보기에 워터마크가 삽입되어 있는지 거의 알지 못하도록 원 데이터의 주파수와 거의 같은 주파수를 삽입하여 보이지 않도록 구조화하는 방법이다.

이 방식은 이미지에 대한 모든 종류의 왜곡 조작에 강하다는 것이 특징이다. 저작자의 기록인 워터마크는 매우 심하게 노이즈가 삽입되거나, JPEG손실압축(10%), 또는 전 이미지의 15%를 삭제하여도 감지가 되는 장점이 있다.

1.2.4 생성 키 값에 의한 워터마킹

삽입하고자 하는 워터마크를 패턴에 의한 키 발생 방법에 의존하는 방법은 워터마크신호가 어떤 패턴의 형태로서 삽입 및 추출되며, 이러한 워터마크 패턴의 생성은 의사난수(Pseudo Random Number) 발생함수를 이용한다. 이 알고리즘은 다른 공간분석 방법들 보다 워터마크가 비교적 견고하며, 이미지의 밝기차이에 의한 워터마크 신호의 공간적인 분포나 이미지의 전 영역에 대한 고른 분포를 하는 기존의 방법들이 받을 수 있는 공격에 대해 강하다.

예를 들어, Fridrich의 알고리즘의 경우 기존 방법의 단점을 보완하기 위해서 워터마크의 패턴을 이미지데이터에 겹치게 하는 방법을 사용하여 이를 극복하였다. 그러나 이러한 방법을 사용할 경우 이미지가 손상될 위험이 있기 때문에 극히 미

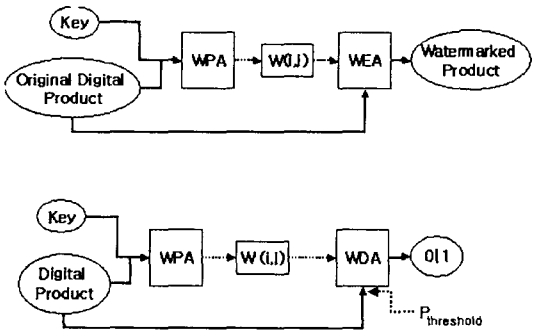

그림 2. 키(ID) 값을 이용한 워터마크 삽입 및 추출 구조

세한 양의 워터마크신호를 삽입해야 하며 이러한 워터마크 생성과 삽입을 위해서 의사난수와 픽셀 단위로 계산을 해서 임계값을 넘지 않도록 조절한다. 그러나 이러한 방법은 너무나 계산량이 많아 비효율적이며 워터마크신호가 단순한 패턴에 의한 의사난수이기 때문에 추출할 경우 임계값이 낮은 워터마크신호에 대한 판별이 어려운 단점이 있다.

2. 개발내용

2.1 워터마킹의 특징

디지털 워터마킹은 개념적으로 투명한 패턴으로 삽입된 이미지로서 워터마크 삽입 알고리즘과 비밀키를 사용한다. 워터마크의 목적은 원 이미지에 대한 부가적인 정보를 이미지의 가시적인 수정 없이 제공하여 파일 포맷의 변화와 같은 필요 없이 음성적으로 날짜 및 시간을 워터마크로 남겨 이를 비교하여 인증하는 방법이다.

이미지에 정보가 가시적인 방법으로 삽입되거나 이미지 포맷과 유사한 헤더에 더해지는 방법은 쉽게 지워지거나 대체될 수 있다. 디지털 워터마크는 이미지에 지속적이고 견고한 방법으로서 비가시적인 형태로 삽입되어야 한다.

워터마크 삽입 처리는 비밀키에 의존하여 키를 소유하고 있어야 하고 숨겨진 워터마크 정보에 접근이 가능하도록 해야 한다. 즉, 키를 이용하여 워터마크를 읽는다. 또한, 해독 또는 감지 알고리즘을 통해 정보를 전달한다.

워터마크의 중요한 특성은 데이터 왜곡에 대한 견고성이다. 이것은 워터마크가 일반적인 이미지 조작을 받은 이미지로부터 읽을 수 있어야 하는 것이다. 예를 들어 필터링, 스케일링, 노이즈 추가, 크로핑 등이다. 워터마크는 저작권 보호, 핑거프린팅, 또는 접근 조작에 대해 안전한 형태로 삽입되어야 한다. 이것은 비밀키를 제외한 삽입알고리즘의 세부사항을 모두 알고 있는 공격자가 워터마크에 대한 공격을 하지 못하도록 해야 한다. 이러한 응용의 경우, 워터마킹 구조는 동기적인 암호화 방법으로 비밀 키 방법을 예로 들을 수 있다. 이러한 디지털 워터마킹의 특성을 요약하면 다음과 같다.

2.2 구성도

인터넷 사용자가 등록을 하게 되면 인증시스템이 인증 키를 부여하고 원 저작물에 저작자의 입력 정보와 사용자의 접속정보를 삽입하여 이후에 저작물에 대한 저작시비를 가릴 수 있다. 그림 3에서 ①~⑨까지의 과정 중 타 시스템은 ③~④가 생략되거나 혹은 미흡한 것이 현실이고 만약 부분적으로 적용한다고 하더라도 PPP접속자에 대한 일체의 적용이 어려운 것이 현실적이다. 접속시에 사용자를 제한하거나 사용자의 이동성을 고려하여 사용인증에 대하여 항시 추적하면서 알려주며 DB화하는 시스템으로 가능한 많이 Hacking으로부터 보호하며 저작권의 보호까지도 같이하고, 이러한 상태를 통한 등록, 확인, 요청, 공급, 반납과 폐기를 신속하게 웹상에서 처리할 수 있다. 한편,

지각적 비가시성 (Perceptual Invisibility)	워터마크 신호는 디지털 데이터의 변경에 의해 삽입된다. 이러한 변경은 인지될 정도로 품질을 저하시켜서는 안된다. 소유자는 변경의 강도를 결정할 수 있다. 많은 변경은 견고하고 높은 정확성으로 검출 가능하지만 상품의 저하를 일으키게 된다.
복잡성 (Complexity)	워터마크 신호는 많은 복잡성에 의해 특성화된다. 이것은 유사한 워터마크의 구성을 피하기 위해 필수적이다. 결국 3자에 의해 워터마크 결정은 더욱 어렵게 된다. 복잡한 워터마크의 다른 이점은 신뢰할만한 통계적 성질을 제공하고 워터마크의 검출은 정확성이 높다는 것을 알 수 있다는 것이다.
워터마크 키 (Watermark Key)	어떤 워터마크 신호는 워터마크 키인 정수(혹은 정수들의 집합)와 관련된다. 이러한 키는 워터마크 k를 생성하고 삽입하고 검출하는데 이용된다. 이러한 키는 기밀이고 전적으로 디지털 상품의 법적 소유자를 특정화한다.
통계적 효율성 (Statistical efficiency)	특정 워터마크의 검출은 적절한 키가 사용되었을 때 성공이다. 각 워터마크는 유일한 키에 대응되어야 한다.
통계적 비가시성 (Statistical efficiency)	동일한 키로 워터마크된 많은 수의 디지털 상품들의 소유는 워터마크를 결정하지 않는다. 동일한 키로 워터마크된 다른 상품들은 서로 다른 워터마크 신호를 전송한다. 3자에 의한 소유자 키의 추출은 불가능함을 주장한다. 가짜의 워터마크 키, 즉 이전에 디지털 이미지에 삽입된 적인 없는 워터마크를 검출하는 것은 결정할 수 없다.
다중 워터마킹 (Multiple watermarking)	연속적인 서로 다른 워터마크 계열을 동일한 이미지에 삽입할 수 있다. 이러한 워터마크 각각은 대응되는 유일한 키를 이용함에 의해 검출가능하다. 저작자는 많은 상품을 워터마킹하기 위해 동일한 키 f를 이용할 수 있다.
견고성 (Robustness)	다양한 종류의 조작은 디지털 상품의 품질을 향상시키거나 크기를 압축하거나 워터마크를 제거하기 위해 디지털 상품에 수행된다. 워터마크들은 동시에 비가시적이고 필터링과 JPEG (MPEG) 압축과 같은 다양한 조작에 견고한 변경을 만들기 위해 효율적인 방법을 이용한다. 따라서 워터마크는 높은 품질을 나타내는 변조된 이미지에서 여전히 검출된다.

사용자 키는 새롭게 인증이 된 상태이고 등록 때만 사용이 됨으로 더 이상 키를 인터넷상에서 전송하지 않아도 된다. Server에 대한 접속상태를 모두 이력으로 남겨서 권한외의 접속시도를 기록관리하고 사용자의 사용 한도 또한 점검을 한다. 이는 다시 말하면 사용자의 한계를 해당 Computer에서 일정한 Group으로 처리하여 구성을 할 수 있도록 한다. 여기서 주목할 것은 이모든 내부형식의 처리가 암호화된 상태로 내부에서 처리를 한다. 웹상의 모든 권한에 대한 상태를 CGI내에서 처리하여 각 사용자별 구성이 웹상태로 지원이 되기에 별도의 인증이 없이 사용자별 워터마킹이 구현되어 표현이 된다.

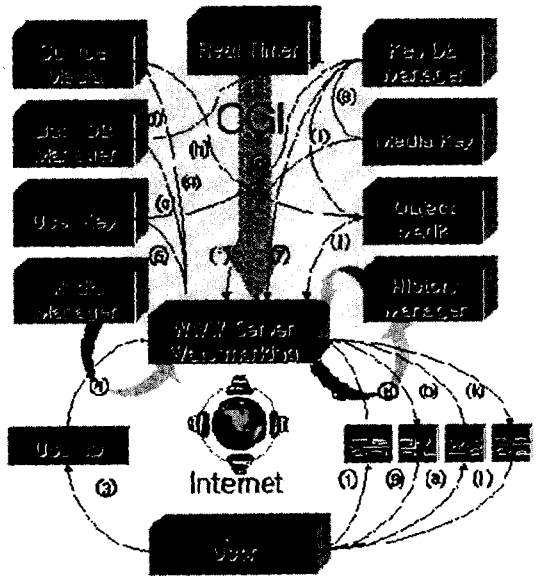

그림 3. 인증시스템 구성도

2.3 워터마크 삽입

워터마크 삽입은 그림 4와 같이 나타낼 수 있다. 워터마크는 사용자 키를 인터넷상에서 취하여 사용자 고유의 키로서 존재하며 등록 처리된 후

사용자로부터 요구된 데이터를 결합하여 워터마킹될 내용을 사용자 키와 함께 암호화 module로 보내면 새로운 키가 생성된다. 여기서 워터마킹될 내용은 사용자 키 외에 내용들이 저장되면 인터넷 상의 사용자에게 공급이 되고 사용자는 아무런 의심 없이 데이터를 사용하도록 한다.

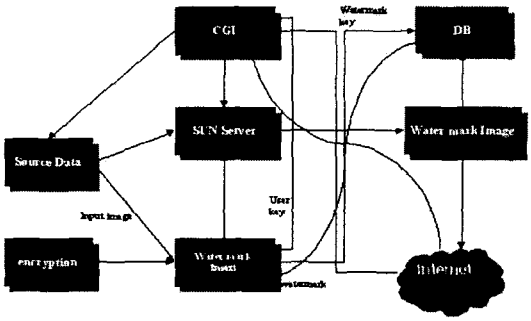

그림 4. 디지털 워터마크 삽입

2.4 워터마크 추출

워터마크 추출은 그림 5와 같이 나타낼 수 있다. 추출과정은 사용자의 접속사항을 이력으로 추출하며 원본 데이터 내에서 기본적인 키를 추출하고 이 키를 이용하여 DB에서 검출 후에 사용자의 키를 이용 워터마크의 모든 이력사항을 처리한다. 워터마킹된 내용을 근거로 DB에서 finger- printing도 추출할 수가 있다.

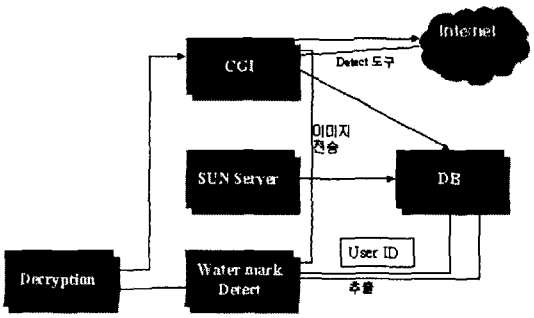

그림 5. 디지털 워터마크 추출

2.5 암호화 방법

워터마크정보를 보호하기 위해서 기본적으로 고려해야 할 사항을 다음과 같이 정리할 수 있다.

- 기밀성(Confidentiality) 보장

암호화된 데이터를 당사자만이 파악할 수 있도록 하는 기능으로 암호화의 가장 기본적인 목표라고 할 수 있다. 이러한 기밀성은 암호화에 사용되는 키 값을 알고 있는 워터마킹 인증 시스템만이 원래의 데이터를 복호화 해낼 수 있도록 하여야 한다.

- 사용자 인증(Authentication) 기능

암호화된 데이터를 다른 사람에게 전송하는 경우에 지켜져야 할 사항으로 사용자 인증 기능을 들 수 있다. 인증 기능이란 전송하는 사용자 입장에서는 수신자가 정당한 수신자인가를 확인할 수 있어야 하며, 수신자 입장에서는 송신자가 정당한 송신자인가를 확인할 수 있어야 한다는 의미이다.

- 무결성(Integrity) 보장

암호화된 데이터를 다른 사람에게 전송하는 경우에 지켜져야 할 사항으로 데이터의 무결성 보장을 들 수 있다. 데이터의 무결성이란 데이터 수신자 입장에서 수신된 데이터가 중간에 변경이 되지 않았다는 사실을 확인 할 수 있어야 한다는 의미이다.

- 부인 봉쇄

역시 암호화된 데이터를 다른 사람에게 전송하는 경우에 지켜져야 할 사항으로 데이터의 송수신 후 송수신자가 자신이 송신하거나 수신한 데이터의 송수신사실을 부인하는 것을 방지할 수 있어야 한다는 점이다.

본 기술개발에서는 상용화로 폭 넓게 쓰이는 DES(Data Encryption Standard)를 사용한다.

DES는 RSA나 PGP와는 달리 저작권료가 없고 리눅스 시스템의 패스워드 루틴이 DES로 되어 있을 만큼 안정성과 신뢰성이 입증되고 있다.

DES 암호 알고리즘에 입력되는 입력 값은 64비트 평문과 56비트 키이다. 키의 사이즈가 56 비트라고는 하지만 실제 크기는 패리티 비트 8비트와 합쳐 64비트이다. 암호화는 세 단계로 이루어진다. 첫째는 64비트 평문이 치환된 입력을 생성하기 위해 비트 열의 순서를 재조정하는 Initial permutation 단계를 거친다. 다음엔 동일한 함수의 16회 반복 단계가 수행되는데 순열이나 치환의 동작이 이루어진다. 16 단계의 반복 함수를 거친 입력은 좌우 32비트가 swapping 되며 마지막으로 Inverse permutation을 통과함으로써 최종적인 64비트 암호문을 얻게 된다.

2.6 인증 시스템의 구현방법

2.6.1 인증키(Encryption) 생성

이미 등록된 사용자의 경우 CGI Manager는 암호키 DB서버로부터 사용자만의 키를 획득한 후에 Onetime password를 생성하며 사용자의 인증형식을 위한 사용자 Control Server에서 횟수 등을 통제 받아서 새로운 인증 키를 부여받는다. 이때 발생되는 Onetime Password는 데이터base의 키값으로 대치가 되며 이의 모든 자료의 근거는 인터넷 원자시계가 대행을 하여 준다.

2.6.2 워터마크 삽입과 인증키(Encryption) 삽입

CGI Control은 워터마크와 인증키를 원 미디어에 삽입한다. 이때 공간영역에서의 워터마크를 기본으로 미디어에 삽입한다. 여기서 생성된 워터마킹된 미디어는 새로운 사용자만을 위한 임시 저장소에 보관이 되도록 한다.

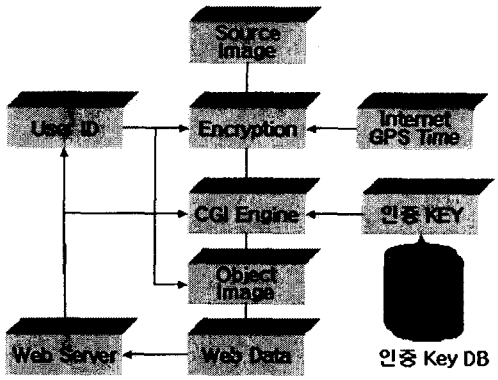

그림 7. 인증키 미디어에 등록

2.6.3 인터넷상의 표현방법 및 사용자 다운로드

CGI Control은 사용자별 임시 저장소에서 자료

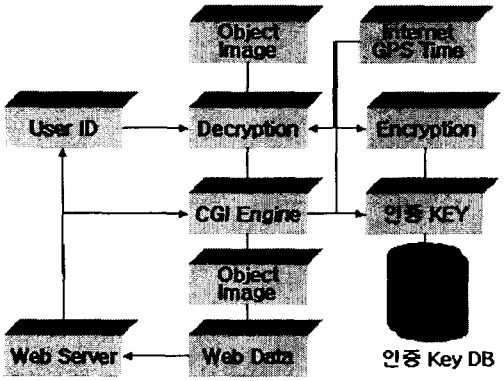

그림 6. 인증키 생성

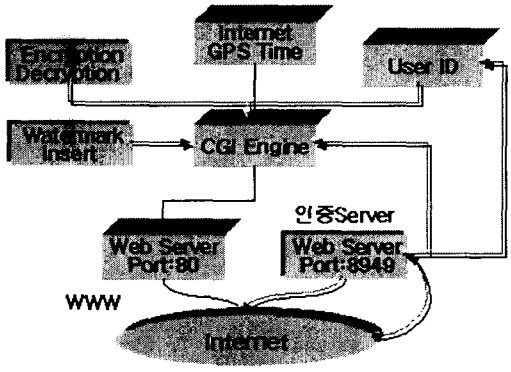

그림 8. 웹 상의 사용자를 위한 다중 미디어

를 처리하도록 구현이 되며, 인증된 사용자만이 워터마크된 미디어를 다운로드 할 수 있다. 이는 인터넷상의 사용자 모두가 같은 웹을 참여하지만 서로 다른 공간의 구성으로 접근하여 미디어를 각자만의 유일한 저작물로서 처리할 수 있다. 그리고 시간대별 접속자의 모든 미디어는 복수로 존재한다.

2.6.4 사용자의 사용허가권 부여 및 반납

사용자는 미디어를 중복 사용이 가능하지만 이는 저작권에 대한 비용 지불에 문제가 발생한다. 이를 방지하기 위하여 사용자의 미디어를 반납하여 사용한도를 새로이 받도록 한다. 이때 반납은 간단하게 이루어지지만 키 Manager는 반납시의 미디어에서 워터마킹된 인증 키를 회수한 후에 회수 DB에 등록하고, 반납 미디어를 폐기하며 폐기미디어의 사용을 철저히 감시한다.

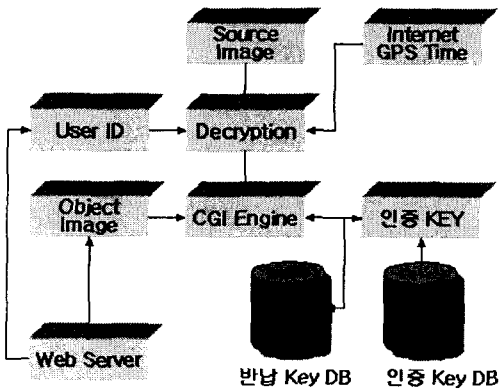

그림 9. 인증 키 반납

2.6.5 사용자별 키 생성 방법론

사용자를 등록할 때 사용자별 키를 생성하도록 사용자 Manager는 키 Manager에 지시한다. 이때 키 Manager는 사용자 Manager로부터 필요한 일부내용으로 전달받는다.

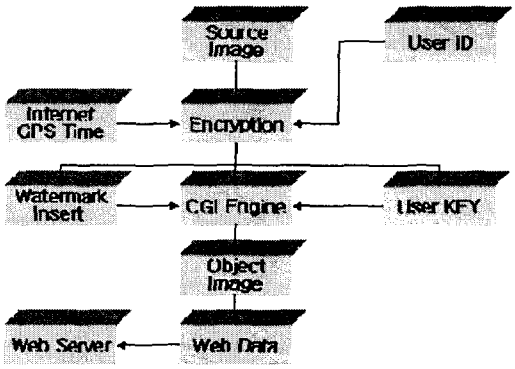

그림 10. 사용자 키 생성

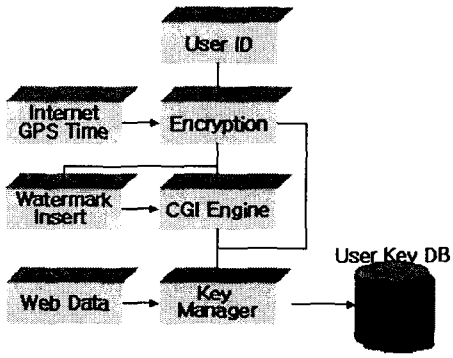

그림 11. 사용자별 키 등록

2.6.6 사용자 등록

웹 서버의 CGI 서버는 사용자 DB에 기본 등록사항을 등록한다.

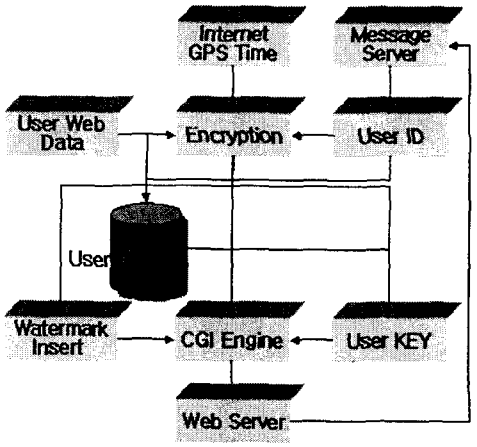

그림 12. 사용자 등록

2.6.7 워터마크 추출과 인증키(Encryption) 검증

사용자의 미디어반납 시 혹은 미디어의 중복 사용 등을 위한 대책으로 우선은 해당 미디어를 웹 서버의 임시 저장소에 모든 자료를 저장한다. 이때 CGI 서버는 모든 키 Manager와 데이터 베이스로부터 인증 키를 사용하여 검증을 완료한다.

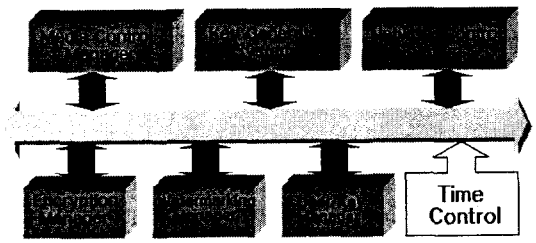

그림 13. 인증 키 검증

3. 개발결과

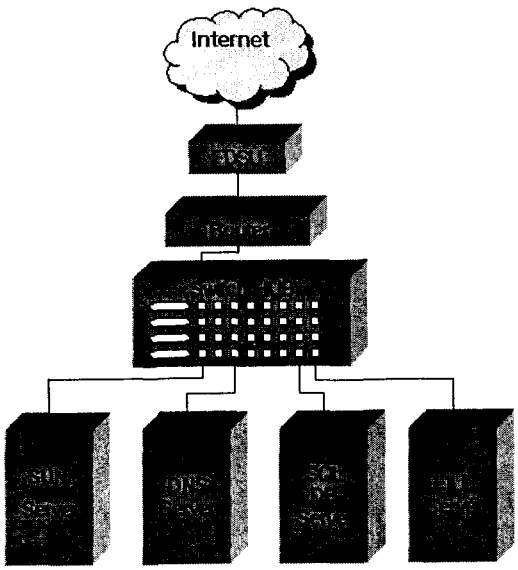

그림 14. 인터넷환경상의 실제구성

3.1 처리방법

본 기술개발은 UNIX 시스템의 웹 서버인 Apache 내에서 운영이 된다. 또한 영상의 변환 작업 후에 워터마킹의 삽입이 이루어지며 이때의 워터마킹은 사용자로부터의 데이터와 CGI Module에서의 서버 상태를 입력받아서 암호화 모듈에 의한 DB 구성으로 각각의 키를 발생하여 워터마크의 데이터와 DB의 Table을 동기화 한다. 이때 발생되는 키와 워터마크내의 데이터는 유일한 값을 갖게 된다.

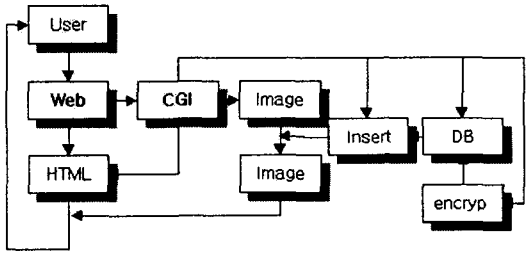

그림 15. 인터넷상의 워터마킹 구성도

3.2 처리순서

- 사용자가 방문할 때 웹 서버는 사용자의 모든 처리상태를 확인하여 DB를 확보
- CGI Control은 DB등록과 영상 워터마크 데이터를 삽입한다.
- 삽입된 영상을 표현하도록 HTML자체가 코드화 된다.
- 암호키를 생성하도록 한다.
- 실제 영상을 HTML과 동기화 되도록 한다.

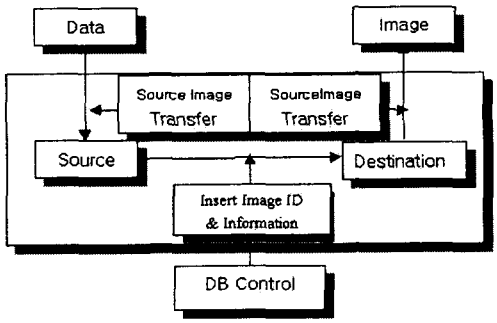

그림 16. 워터마킹 Module

3.3 시스템 개발 환경

- 웹 서버 : Apache
- 시스템 : Sun Ultra 5
- CGI : C & Perl
- Graphic Format : RGB Raw 데이터, GIF 데이터
- Graphic Tool : ImageMagick
- Encryption : DES
- Database : Oracle 8.0i
- 웹 데이터 : HTML& JAVA script

3.4 사용자 적용

Sun Ultra 5에 웹 서버인 Apache와 Oracle8.0i DB를 설치하여 기본적인 운영환경을 구성하고, 사용자 화면의 구성으로 인증을 받기 위한 Graphic 화면의 설계를 한다. 이때 설계되는 화면 구성은 각기 다른 CGI로 구성이 되어 HTML간의 통신을 POST에 의해 처리되도록 한다.

사용자는 필요로 하는 영상 또는 각종 자료를 요청하며 이때 요청 시 받아들인 서버는 CGI를 이용하여 사용자의 자료를 접수하여 인덱스키를 생성하고 서버자체의 키 생성 시스템과의 자료를 비교하여 DB를 생성한 후에 워터마킹될 데이터를 생성하여 사용자의 요구 자료에 워터마킹을 하고 이 자료는 웹 서버를 통하여 사용자에게 공급된다.

3.5 실험결과

3.5.1 전용브라우저에서의 워터마킹 처리

전용브라우저를 사용할 경우 워터마킹 기술을 구현하기 위한 직접적인 도구로써 활용이 가능하고 범용 브라우저에서 제공하지 않는 워터마킹 정보표현을 위한 다양한 기능을 부가할 수 있다. 자체 개발한 전용 브라우저를 사용하는데 있어 그림 17, 그림 18에서처럼 우선 홈페이지 프레임 영역을 먼저 구분하고 선택된 프레임 내부의 이미지를 워터마킹하기 위해 선택한다.

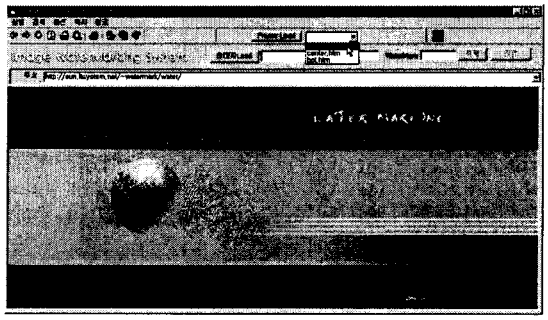

그림 17. 웹 page상의 프레임 구분

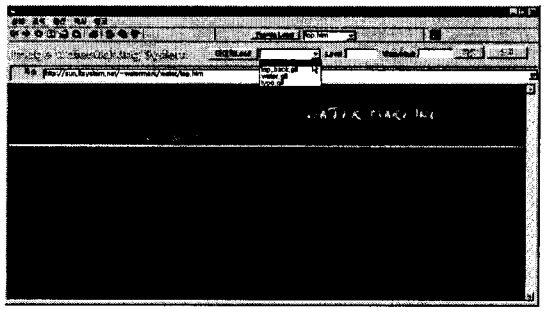

그림 18. 선택된 Top 프레임

웹페이지 상에서 프레임으로 구분한 후 상단 메뉴의 기능 키 중 "Frame Load"버튼을 누르면 프레임 내부에 포함되어 있는 HTML을 파악하고

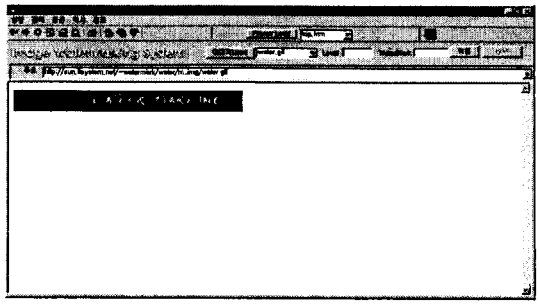

그림 19. 프레임 내에 있는 이미지 선택

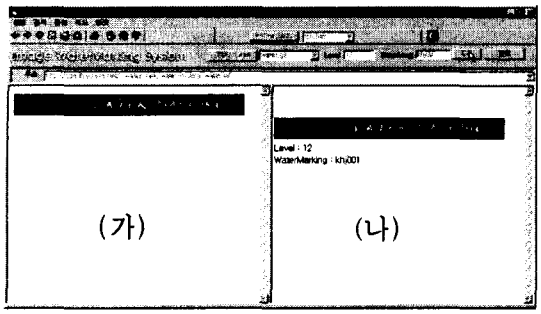

그림 20. 선택한 이미지에 워터마킹 삽입

다시 그 내부에서 이미지 파일을 검출한 뒤 워터마킹할 이미지 하나를 선택하면 그림 20의 (가)화면에 이미지가 나타난다. 그림 20에서 워터마킹에 필요한 레벨과 워터마크를 입력한 뒤 "적용" 버튼을 누르면 워터마크된 이미지와 레벨, 워터마크의 내용이 그림 20의 (나)에 나타난다.

3.5.2 결과영상물

기술개발의 결과 영상물을 그림 21, 22, 23에 나타냈다.

그림 21의 원 영상에 워터마크를 삽입한 영상이 그림 22에 나타나 있으며, 두 영상의 차 영상인 워터마크를 그림 23에 나타내었다. 그림 23의 워터마크는 결과론 적인 의미를 나타내며 삽입 위치나 형태는 영상의 크기, 색상에 좌우된다.

그림 21. 원 영상

그림 22. 워터마킹 영상

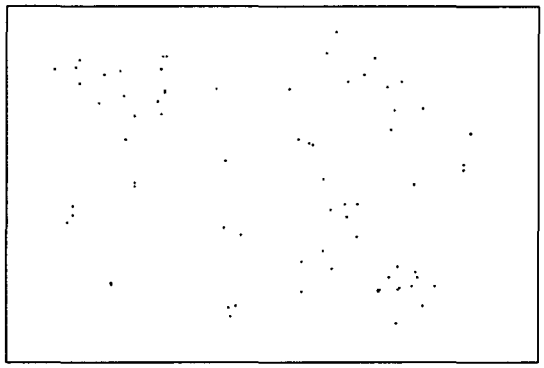

그림 23. 영상내의 워터마크 분포

3.5.3 워터마킹 시험분석

워터마킹을 함에 있어 간과하기 쉬운 것 중에 하나는 SNR(신호대잡음비)와 영상 압축율을 들 수 있다. 아래의 그림 24는 원 영상과 워터마킹 영상에 대하여 JPEG 압축을 수행한 경우, 초래되는 화질의 저하를 나타내고 있다.

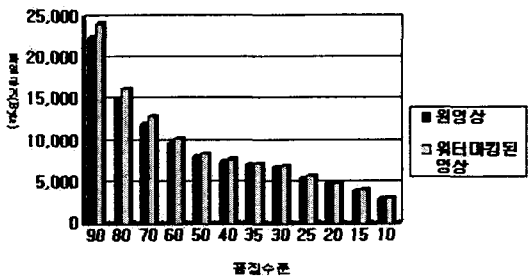

그림 24. JPEG 압축시 파일크기의 변화

워터마크가 삽입된 영상을 품질 수준 90으로 JPEG 압축을 수행한 경우에는 약 31.71dB의 SNR이 측정되었다. 이것은 원 영상을 품질 계수 90으로 JPEG압축을 수행한 경우보다 약 6.48 정도의 SNR이 저하된 것이다. 그림 24를 보면 원 영상에 대해서 JPEG 압축을 수행할 때 SNR의 저하가 급격하게 발생되는 것은 압축에 의해 영상 내에 중복되는 부분들이 사라져 버리기 때문이다. 그러나, 워터마크가 삽입된 영상은 이미 품질 수준에 의해 워터마크 삽입시 영상 내에 중복성이 사라져 버림으로써 SNR의 저하가 그다지 발생되지 않는다. 이것은 제안 방식에 의해 워터마크가 삽입된 워터마킹 영상은 JPEG 압축의 영향을 받지 않음을 의미한다.

아래의 그림 25는 원 영상과 워터마크된 영상과의 압축률 비교를 나타낸 것인데, JPEG으로 압축된 압축파일의 크기가 원 영상보다 크게됨을 알 수 있다. 이것은 워터마크 삽입에 의해 영상 내에 존재하였던 중복성이 감소되면서 압축율에 영향을 주기 때문이다.

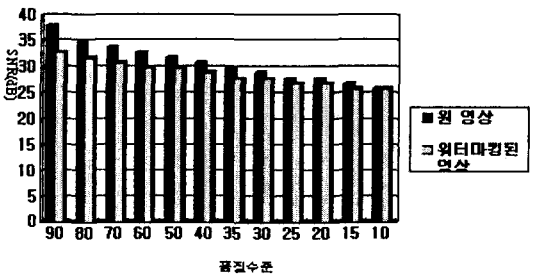

그림 25. JPEG 압축 후의 SNR 변화

이와 같이 워터마킹 영상에 대해 압축파일의 크기를 최소화하는 것이 개발기술의 향후 과제이다.

4. 활용 및 응용

인터넷 기술이 하루가 다르게 발전하면서 그에 따라 인터넷 사용자가 급증하고 생활과 문화의 중심이 인터넷으로 기울면서 이제는 인터넷이 사회의 일부분이 아니라 커다란 문화공간으로 자리잡혀가고 있다.

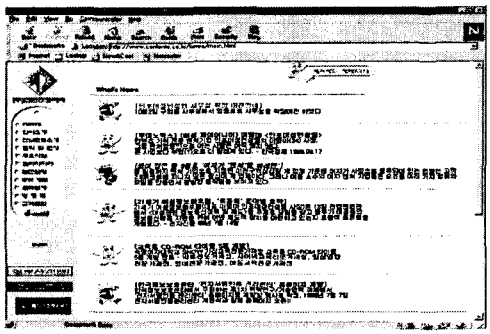

그림 26. 워터마킹된 이미지의 응용

그만큼 인터넷 활용의 중요성이 강조되면서 그에 따른 컨텐츠 보호와 저작권 주장이 강하게 대두되고 있다. 본 "멀티미디어 컨텐츠 보호를 위한 워터마킹 시스템" 기술 개발은 그러한 요구에 부응해 영상, 음성, 사진, 사운드 등 컨텐츠 전반에 걸쳐 보호와 은닉 기술로써 적용하게 된다.

4.1 영상 매체

많은 시간과 노력으로 만들어진 디지털 영상 매체가 어느 순간 타인에 의해 조작, 훼손, 배포,

그림 27. 영상 매체물

판매 등의 권리를 주장한다면 현재로선 대응할 방법이 없다.

본 기술개발은 디지털 영상, 사진, 그림, 상표 등에 워터마크를 삽입하여 전세계 어디서나 제작자의 저작권을 주장할 수 있다.

4.2 음반매체

현재 디지털 컨텐츠 분야에서 가장 논란이 되고 있는 분야가 음반 저작권 시비이다. 어떤 음반이라도 인터넷을 통하면 모두 구할 수 있기 때문에 항상 음반 제작사들과 논란의 대상이 되고 있다.

본 기술이 내세우고 있는 워터마킹 기법은 영상뿐만 아니라 음반, 음성, 사운드에도 적용되어 그 시비를 가려 줄 수가 있다. 누가 언제 만든 음반이며 소유권이 누구인지 그리고 유통경로까지 디지털 마킹으로 밝혀낼 수가 있다. 뿐만 아니라, 역사적인 녹취록의 진위여부도 가릴 수 있어 응용범위가 광범위하다.

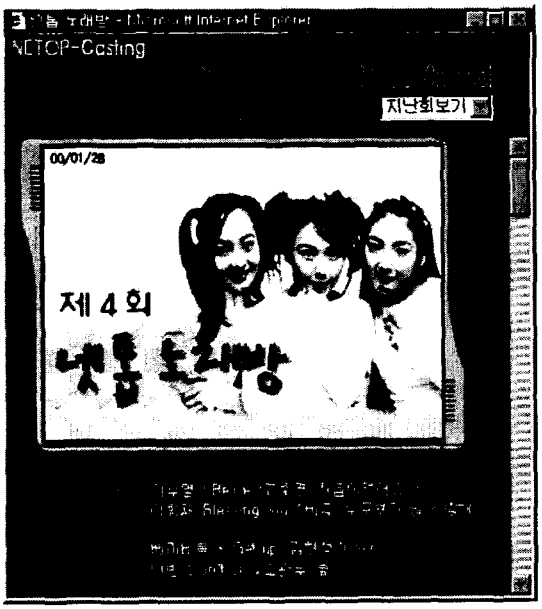

그림 28. 음반매체

4.3 전자도서/출판

음반 매체만큼이나 저작권시비가 강조되는 분야가 전자도서/출판분야이다. 저작자의 동의나 허락 없이 특정 도서, 출판물을 복사, 판매하는 행위에 대해서 저작권을 주장할 수 있다.

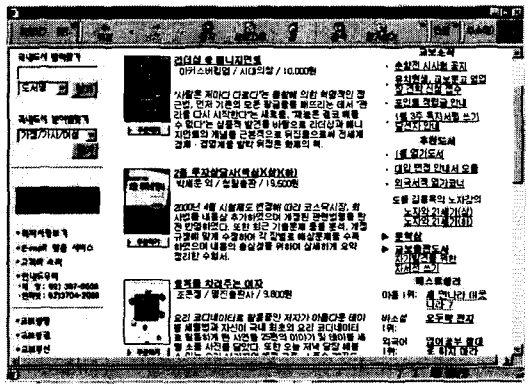

그림 29. 전자 도서

4.4 원격강의

인터넷이 활성화되면서 웹 환경에서의 원격강의도 활발하게 진행되고 있다. 강사의 육성과 강의교재도 워터마킹 기술을 적용하여 저작권 시비를 가릴 수 있다.

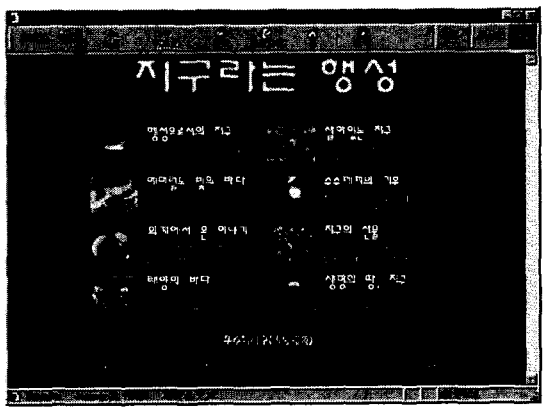

그림 30. 원격강의

4.5 전자상거래

인터넷 사업분야에서 현재 두드러지게 발전하고 있는 분야는 바로 전자상거래 사업이다. 유통상에 신뢰성, 안전성이 보장되면 지금보다 훨씬 더 활성화 될 것이며 거래규모도 많이 증가할 것이다. 전자상거래는 인터넷사업의 대표적인 사업형태로서 인터넷상에서 워터마킹기술로 보호된 실물정보나 음성정보를 가지고 가상의 공간에서 실제 상업적 행위를 할 수 있다.

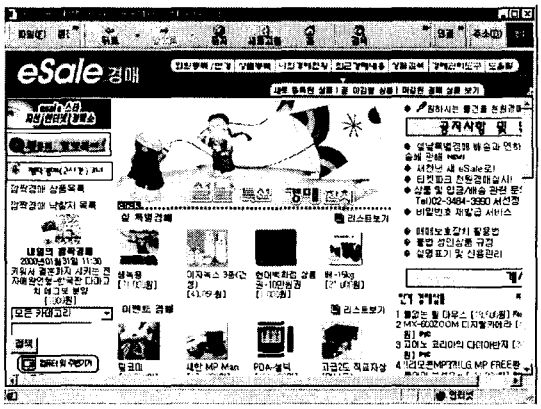

그림 31. 전자상거래

4.6 인터넷 방송

전자상거래 사업만큼이나 잠재력이 있고 성장

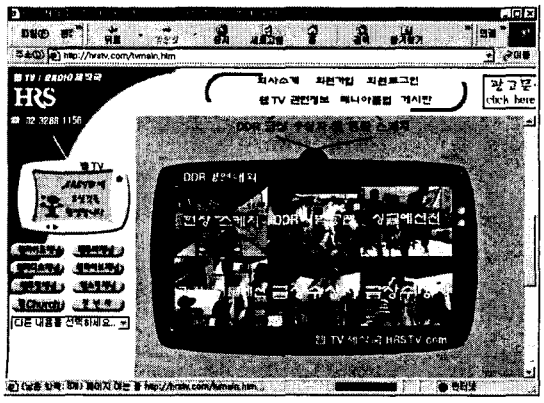

그림 32. 인터넷방송

가능성이 있는 사업분야가 인터넷 방송이다. 인터넷 방송은 멀티미디어 보도 자료와 VOD전송 매체 등을 다루는 디지털 산업의 종합형태이며, 실시간적인 요소가 많이 작용한다. 따라서 정보의 정확성이나 신뢰성이 무엇보다 강조되기 때문에 본 기술개발의 워터마크 삽입기술이 크게 요구되고 있다.

참 고 문 헌

[1] J.J.K O Ruanaidh, F.M. Boland and O.Sinnen : Watermarking Digital Images for Copyright ProtectionIEEE Proc. Vis. Image Signal Processing. Vol. 143, No. 4, pp.250-256, 1996

[2] Kwang-Su LEE, A Watermark for Authentication and Data Integrity12/18/1998 http://monami.kaist.ac.kr/~guspin/report/cs540/Watermark.html

[3] P.W. Wong, "A public key Watermark for image verification and authentication" In Proceedings of ICIP, Oct. 1998

[4] Mi-Suk Chung, Bong-Kyun Rhim, Jeong-Ho Park, Byung-Ha Hwang, Jae-Ho Choi, and Hoon-Sung Kwak : Development of Efficient Wavelet Algorithm for Image CodingKorea, sep, 1997, 電子工學會論文誌 第34卷 S編 第9號

[5] Ingemar J. Cox, Joe Kiliant, Tom Leighton and Talal Shamoon : Secure Spread Spectrum Watermarking for Multimedia IEEE Trans. on Image Processing, 6,12, pp.1673-1687, 1997

[6] R.E. Frazier : Data Encryption Techniquesin http://www.catalog.com/sft/encrypt.html9/7/1999

[7] RSA Laboratories : A Free Cryptographic Toolkit General Information in http://www.epm.ornl. gov/~dunigan/rsaref.txt April 15, 1994

[8] Matthew Fischer : How to implement the Data Encryption Standard(DES) in ftp://ripem.msu.edu/pub/crypt/docs/des-algorithm-details.txt November 1995

[9] Fabien A.P. Petitcolas and Ross J. Anderson : Evaluation of copyright marking systems IEEE Multimedia System 99, vol. 1, pp.574-579, 7-11 June 1999, Florence, Italy, May 1996
[10] Jack Lacy, Schuyler R. Quackenbush, Amy Reibman, James H. Snyder Intellectual Property Protection Systems and Digital WatermarkingAT&T Labs Research Florham Park. NJ; Red Bank. NJ, 31 April 1998
[11] Joshua R. Smith and Barrett O. Comiskey : Modulation and Information Hiding in Images Published in Proceedings of the First Information Hiding Workshop, Isaac Newton Institute, Cambridge, U.K., May 1996. Springer-Verlag Lecture Computer Science Volume 1174.
[12] Davis Pan : A Tutorial on MPEG/Audio CompressionIEEE Multimedia Journal, Summer 1995 issue
[13] R.B. Wolfgang, C.I. Podilchuk, and E.J. Delp, "Perceptual Watermarks for Digital Images and Video", submitted to the Proceedings of the IEEE, 1998.
[14] Elementary Number Theory UIC Honors Seminar in Cryptography, 1997 http://raphel.math.uic.edu/~jeremy/crypt/math.html
[15] Raymond B. Wolfgang, Cristine I. Podilchuk, and Edward J. Delp : Perceptual Watermarks for Digital Images and Video in Bell Laboratories, Lucent Technologies, Murray Hill, New Jersey 1998
[16] 경상현 : Modern Cryptology in ETRI 1995
[17] Clay Irving : Perl : OREILLY SOFTWARE 1997
[18] Herbert Kelly : Oracle 8.0i : ORACLE 1998

이 영 아

• 1993년 이화여자대학교 대학원 사범대학 졸업(석사)
• 1998년~현재 (사)여성정보문화21 이사
• 1999년~현재 한양대학교 대학원 교육공학과 박사과정
• 1999년~현재 21세기여성정보화포럼 대표
• 2000년~현재 한국걸스카우트연맹 정보화 자문위원
• 2000년~현재 중소기업중앙회 여성특별위원회 위원
• 저 서 : 멀티미디어 컨텐츠 기획, 전자상거래, 인터넷 정보검색사 등
• 수상경력 : 여성특별위 위원장 장관급 표창 수상, 중소기업 신지식인상 수상
• 관심분야 : 인터넷, 컨텐츠보호기술, 전자상거래, 멀티미디어 컨텐츠

하 재 호

• 1988년 명지대학교 전기공학과 졸업
• 1996년 (주)콤텍시스템 MIS 개발팀장
• 1998년 I.T. System 대표
• 2000년 고려대학교 대학원 컴퓨터공학과 졸업
• 1999년~현재 (주)컨텐츠코리아 이사
• 2000년~현재 (주)컨텐츠코리아 기업부설연구소 소장
• 관심분야 : 컨텐츠보호기술, 해커추적시스템, 멀티미디어 시스템, 무선통신