정보은닉을 위한 스테가노그라피와 DRM

김 영 실* 박 성 진**

◈ 목 차 ◈

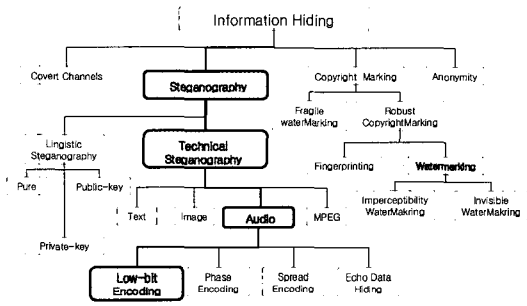
1. 서 론

본 연구에서는 비약적으로 발전하는 컴퓨터 분야에서 온라인과 오프라인에서 정보의 은닉이나 Copyright Marking, 인증 등을 통해 중요한 정보에 대한 보안의 한 방법으로 응용되고 있는 스테가노그라피 방법에 대해서 논의하고 이를 응용하여 정보의 파괴나 잘못된 사용을 예방하고자 한다.

디지털 환경에서의 많은 정보들은 네트워크나 인터넷을 통해 공유되어 사용되고 있다. 이러한 환경에서 정보들은 무단 복사나 사용인가에 대한 허락 없이 유통되고 또는 정보의 정확성에 관계없이 무책임하게 복사되어 사용되고 있다. 디지털 환경에서 정보의 보안은 정보를 안전하게 관리하는 것도 하나의 방법이지만 다른 한편으로는 정보를 은닉하므로 써 불필요한 유출이나 잘못된 사용을 미리 예방하는 것도 필요하다. 그림 1은 정보은닉의 부류를 나타낸 것이다.

정보은닉을 여러 분야에서 응용하고 있으며, 특히 인터넷과 네트워크 공유에 의해 발생하는 정보 공유에 대한 대비책으로 스테가노그라피나 저작권 분야 등에서 유용하게 응용되어지고 있다.

2. 스테가노그라피



(그림 1) 정보은닉의 분류

"Covered Writing"의 뜻을 가지는 그리스어로부터 유래된 것으로 통신상의 두 주체인 송신자와 수신자 사이의 메시지가 제 삼자에게 의심을 받지 않도록 교묘히 숨기는 기법으로 제 삼자가 평범한 일반 메시지 안에 비밀 메시지가 존재한다는 것을 알지 못하도록 숨기는 것을 목적으로 한다.

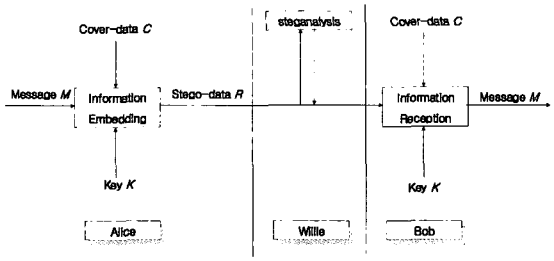
문서로 기록된 최초의 스테가노그라피는 기원전 5세기 그리스의 왕 Histiaeus가 Darius 왕의 죄수로 잡혀 있을 때, 그는 양아들에게 비밀메시지를 전달하기 위하여 노예 머리를 깍아 그 머리에 메시지를 문신한 후 노예의 머리가 길게 자라자 노예를 Miletus로 보내서 메시지를 전달하였다. 또한 고대 로마인들은 과일쥬스, 소변, 우유와 같은 물질을 기반으로 하는 잉크를 이용하여 편지를 쓰기도 했다.

또한 독일인들은 세계2차대전 동안 "마이크로도트"라는 것을 창안해서 사용하였다. 마이크로 도트는 숨

* 대림대학 컴퓨터정보계열 조교수
** 한신대학교 컴퓨터정보통신학부 조교수

기고자 하는 비밀 메시지를 점 하나의 크기로 축소한 후 영문자 i 나 마침표등에 사용하여 많은 양의 비밀 데이터를 전송하는 기법으로 러시아의 국제 우편 검열제도나 미국과 영국의 꽃 반입 금지법등이 바로 전쟁기간동안에 사용되었던 스테가노그라피의 적용 예이다.

현재 가장 이슈가 되는 스테가노그라피 기술들은 디지털 환경을 기반으로 한 기술들이다. 이러한 기술은 1983년 Simmon이 발표한 죄수 문제로부터 발전되어 왔다 .



메시지(마스크)	숨기고자 하는 비밀 데이터
원본	정보가 은닉되기 전 데이터
스테고데이터	원본에 메시지가 삽입된 결과의 데이터
키	메시지의 삽입 및 검출에 사용되는 비밀 정보

(그림 2) 스테가노그라피의 데이터 흐름도

죄수문제 시나리오는 감옥에 갇힌 앨리스와 밥이 감옥에서 탈출하려고 하는 계획을 세운다는 것으로 그들의 모든 대화는 윌리라는 감독자에게 모두 감시되며 만약 윌리가 암호화된 메시지를 발견하게 되면 그들은 독방에 가두게 된다. 그래서 그들은 무해한 것으로 보이는 일반 문서에 비밀 메시지를 숨겨야만 한다.

스테가노그라피는 비밀 통신을 하기 전에 송신자와 수신자사이에 미리 공유되어야 하는 정보가 무엇이냐에 따라 순수 스테가노그라피, 비밀 키 스테가노그라피, 공개 키 스테가노그라피 그리고 비밀통신에서 전송되는 정보를 공격자가 처리할 수 있는 능력을 기준으로 공격자 모델을 수동적인 감시(passive-Warden), 능동적인 감시(active-Warden), 악의적인 감시(malicious-Warden)로 나눈다.

○ 순수 스테가노그라피

비밀 통신을 하기 위해 송신자와 수신자가 서로 어떠한 정보도 공유하지 않아도 되는 기술로 가장 이상적인 형태로 구분되지만 설계하는 것이 어렵다. 실제로 송신자 또는 수신자가 감시자와 송·수신자가 구분할 수 있는 사전 인증정보 또는 식별정보가 없기 때문에 전송되는 정보에 비밀 메시지가 숨겨져 있다는 것을 알 수 없다. 이러한 이유때문에 일반적인 스테가노그라피에서는 비밀 데이터를 이용하여 통신하기 전에 송신자와 수신자가 서로 어떤 정보를 공유하고 있다는 가정하에 설명된다.

○ 비밀 키 스테가노그라피

스테가노그라피에서 사용하는 키의 비밀성에 의존하는 기술이다. 이는 비밀통신을 하기위해 송신자와 수신자가 사전에 비밀 키 또는 공개키를 공유하는 기술로, 가장 일반화되어 사용되는 기술이다. 이 방법이 가지는 장점은 의사난수 키스트림을 만드는데 사용되는 공유된 키를 쌍방이 모두 가지고 있다는 것이다. 실제 네트워크상의 공격자들은 비밀 메시지가 숨겨져 있는 스테고데이터를 보고 아무런 변화를 느낄 수 없기 때문이다.

○ 공개 키 스테가노그라피

공개 키 방법에서는 비밀 통신을 위해 송신자와 수신자가 미리 비밀키를 공유할 필요 없이 암호기술로 공개된 상대방의 공개키로 비밀 통신을 할 수 있는 기술이다.

비록 감시자가 전송되는 데이터의 패리티 비트를 검사하더라도 얻어진 결과로부터 비밀 메시지를 복호화 할 수 없기 때문에 안전하다고 할 수 있다. 수신자는 전송된 스테고데이터를 검출 알고리즘의 입력으로 넣어 결과를 얻은 후 이 결과의 패리티비트 값과 자신이 가지고 있는 비밀 키를 복호화 알고리즘의 입력으로 사용하면 비밀 메시지가 검출된다. 전송된 데이터에 비밀 메시지가 존재하는지 존재하지 않는지를

알 수 없기 때문에 수신된 데이터에 대하여 매번 추출과 복호화를 수행해야하는 문제점을 가지고 있다.

다음은 스테가노그라피의 기술과 그것을 공격하는 공격자들에 대한 것을 비교한 표이다.

(표 1) 스테가노그라피 비교

	공유 정보	안전성	공격자 모델	문제점
순수 스테가노그라피	없음	삽입 및 추출 알고리즘	수동적	실례가 없음
비밀 키 스테가노그라피	비밀 키	키 또는 cover	수동적	사전에 키 공유
공개 키 스테가노그라피	공개 키	키	능동적	비밀 정보 존재의 유무를 결정하기 어려움

(표 2) 스테가노그라피 공격자 비교

	능력	사전 정보	공격 목표
수동적	관찰	없음	비밀 통신 감지
수동적	약간의 변형	삽입 및 추출 알고리즘	비밀 통신 방지
능동적	변경 및 다른 사용자로 가장가능	삽입 및 추출 알고리즘	비밀 통신을 유도하여 비밀 통신 방지

3. 다양한 스테가노그라피 구현 방법들

스테가노그라피는 정보은닉을 위해 사용되는 매개체가 어느 것이냐에 따라 여러 가지 방법으로 구별할 수 있다.

3.1 텍스트 스테가노그라피

가장 오래된 스테가노그라피 기술로 요즘에는 작가에게 로열티를 지불하지 않고 문서의 동일한 복사본을 만들어 사용하는 것과 같은 넓은 범위의 프라이버시 침해를 방지하기 위해 사용자의 눈에 띄지 않는 유일한 코드를 문서에 마킹하는데 사용된다.

이 기술은 기본적인 보안 방법과 관련하여 사용되도록 권고되고 있으며, 포토카핑과 같은 방법에 의해 왜곡되지 않으므로 복사된 문서를 추적할 수 있다. 이러한 마킹 기술은 문서나 포스트 스크립트 또는 텍스트 파일과 같은 문서형태의 파일에 이미지를 표시하는 방법이 적용되며, 코드가 문서 본문의 형태로 변환되어 문서에 삽입된다.

이것을 가능하게 해주는 기본적인 엔코딩 기술은 라인 이동 코딩(Line-Shift Coding), 워드 이동 코딩(Word-Shift Coding) 등이 있다.

○ 라인 이동 코딩

이 방법은 문서를 유일하게 인코딩하기 위해 문서 라인들을 수직으로 이동시키는 방법이다. 인코딩과 디코딩은 문서파일 또는 페이지 이미지 비트맵에 일반적으로 모두 적용되며, 문서의 모든 두 번째 라인을 이동시키기 때문에 1/300Inch가 올라가거나 내려가므로 가장 명백히 표면적으로 드러난다.

○ 워드 이동 코딩

이 방법은 단어와 단어사이의 간격을 조절하여 코드를 인코딩하는 방법으로 문서파일 또는 페이지 이미지 비트맵에 일반적으로 모두 적용시킬 수 있다. 단어 사이의 간격이 조절된 것이므로 숨겨진 마스크를 찾기 위해선 단어와 단어사이의 간격이 조절되지 않은 문서가 필요하다. 스테가노 데이터를 살펴보면 단어와 단어사이를 아주 크게 또는 아주 작게 되어 있는 부분을 찾을 수 있을 것이며 이 간격을 조절하여 숨겨진 메시지인 마스크 데이터를 찾는다. 이 방법이 라인 이동 코딩 방법보다는 은닉의 가능성이 높다.

3.2 이미지 스테가노그라피

강력한 그래픽을 지원해주는 컴퓨터와 소프트웨어의 발달로 최근 몇 년간 가장 빠르게 성장한 기술이

바로 이미지 스테가노그라피다. 이 방법은 HVS(Human Visual System)에서 인간이 구분할 수 있는 색에는 제한이 있다는 사실에 근거한 기법으로, 어떠한 형태의 데이터라고 하더라도 이미지의 비트 스트림에 은닉할 수 있다.

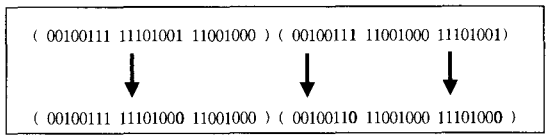
컴퓨터에서 이미지는 다양한 포인트 또는 픽셀로 명암의 밝기를 표현한 배열이다. 이러한 픽셀들은 이미지의 라스터 데이터로 구성된다. 또한 디지털 이미지들은 특히 픽셀 파일마다 24-비트 또는 8비트로 저장된다. 이중 24비트 이미지를 트루 컬러 이미지라고도 하며 정보를 숨길 수 있는 더 많은 공간이 제공되는 이미지이다. 비록 정보를 숨길 공간이 적게 제공된다 하여도 8-비트 컬러 이미지들도 정보를 숨기기 위하여 이용되고 있다. gif와 같은 8-비트 컬러 이미지에서는 각각의 픽셀을 한 바이트로 다시 표시하며, 이때 픽셀의 값은 0-255사이의 값을 가진다. 8-비트 이미지에 비밀 정보를 은닉하려고 할 때는 팔레트와 이미지를 고려해볼 필요가 있다. 또한 이 기술을 할 때는 원본 데이터로 Mona Lisa와 같이 잘 알려진 이미지는 사용하지 않는 것이 좋다. 또한 단일 컬러가 넓은 영역을 차지하고 있는 이미지는 삽입된 데이터에 의해 생성된 변화를 알아보기 쉬우므로 되도록이면 선택하지 않는 것이 좋다.

이미지 스테가노그라피가 가능하도록 해주는 엔코딩 기술은 LSB(Least Significant Bit Insertion), 마스킹과 필터링, 알고리즘 그리고 변형(Transformations) 등이 있다.

○ LSB(Least Significant Bit) 삽입

LSB 삽입은 제공되는 방법 중 가장 잘 알려진 방법으로 가장 적게 나타난 비트에 메시지 비트를 삽입하는 기법으로 이미지가 gif나 bmp 형태에서 jpeg와 같은 손실압축 형태로 변경되면 이미지에 은닉된 데이터가 파괴될 수 있다는 문제점을 가지고 있는 방법이다.

픽셀 비트값의 변화는 사람의 눈으로는 확인할 수 없기 때문에 24-비트 이미지 각각의 바이트에 LSB 방법을 적용할 때 각각의 픽셀을 세 바이트 형태로 표현할 경우 각각의 픽셀안에 3-비트를 인코드 시킬 수 있다. 다음 그림 3는 24-비트로 구성된 원본 이미지의 binary 값에 10000011이라는 코드 값을 갖는 문자 "A"의 binary 값을 삽입시킨 예이다.



(그림 3) binary 스트림에 정보를 삽입한 예

위와 같이 이진 스트림에 숨기려고 하는 데이터의 이진 코드를 삽입하였다 하여도 실제 사람의 눈에는 원본 이미지의 이진 스트림이 변경되었다는 것을 알 수 없다.

만약 8-비트 이미지에 LSB 기술을 적용하려고 한다면 24-비트 형태의 이미지와 같이 처리가 되지 않고 팔레트에서 다른 팔레트로 변경되는 경우가 발생하므로 주의해야 한다. 또한 인접한 팔레트의 색상이 비슷하지 않다면 원본 데이터에 왜곡이 심해질 수 있기 때문에 주로 grayscale 이미지 사용하고 있다.

○ 마스킹과 필터링

마스킹과 필터링은 종이에 워터마크하는 것과 유사한 방법으로 이미지에 마킹하여 정보를 은닉하는 방법이다. 워터마킹은 이미지에 통합되는 기술이기 때문에 실제 손실 압축으로 인한 이미지 변형을 염려하지 않고 적용할 수 있다는 장점을 가진다. 하지만 기술적으로 스테가노그라피는 이미지안에 있는 데이터를 다루는 것이므로 워터마킹과는 다르다고 할 수 있으며, 손실 압축인 jpeg 이미지에 적용하기 적합한 기법으로 알려져 있다.

3.3 오디오 스테가노그라피

통신이 발전하면서 서로 다른 음악 파일을 전송해서 공유하는 경우가 많다. 또한 음악 파일은 HAS(Human Auditory System)에서 일정한 영역을 벗어나는 음은 사람이 구분하지 못한다는 특성을 가지고 있다. 그러므로 오디오 파일에 메시지를 숨길 수 있다면 쉽게 비밀 정보를 전달 할 수 있는 기술이다. 즉 오디오 파일의 잉여 잡음에 숨기고자 하는 비밀 메시지를 삽입해도 음악을 듣는 청취자는 변화를 느

낄 수 없다.

오디오 스테가노그라피가 가능하도록 해주는 기법은 하위비트 엔코딩(Low-Bit Encoding), 위상 엔코딩(Phase Encoding), 스프레드 스펙트럼(Spread Spectrum), 에코 데이터 은닉(Echo data hiding)등이 있다.

○ 하위비트 엔코딩

하위비트 엔코딩 기법은 다른 데이터 구조에 데이터를 삽입하기 위한 가장 간단한 방법으로 이진 스트림으로 샘플링된 비트의 마지막 비트를 숨기고자 하는 비밀 데이터로 대체한다. 이 방법은 오디오 시그널에 큰 크기의 데이터를 인코딩할 수 있다. 하지만 송수신 채널의 잡음이나 리샘플링, 압축등의 일반적인 신호처리 시 은닉된 데이터를 필터링하기 어렵다.

일반적으로 잡음이 없는 채널의 경우 용량은 1kHz 마다 1kbps이다. 즉 비트률은 8kHz 로 샘플링된 스트림에 8kbps가 된다.

○위상 엔코딩

위상엔코딩은 초기 오디오 세그먼트의 위상을 데이터를 표현하는 연관된 위상으로 바꾸는 방법이다. 결과 세그먼트의 위상은 세그먼트 사이에 관련된 위상을 유지하기 위해 조정되며 시그널과 감지할 수 있는 잡음 사이에 효과적인 코딩 방법 중에 하나이다. 하지만 마스크를 필터링하기 위해 주파수 영역의 길이와 시작 위치점을 파악해야 하며, 마스크 필터링 시 사용되어진 매개체인 원본 데이터가 필요하다.

○스프레드 스펙트럼

대부분의 통신 채널은 대역폭을 보존하기 위해 가능한 한 스펙트럼의 정밀한 영역에 오디오 데이터를 집중시킬 수 있다는 특성을 이용한 방법으로 자연 잡음이나 고의적인 전파 방해에 강한 면을 가지고 있다. 확장된 스펙트럼 기술을 이용할 때 엔코딩된 데이터는 가능한 한 빈번하게 스펙트럼을 통하여 나타나게 된다. 디지털 워터마킹에서 기반 기술로 이용되고 있다.

○ 에코 데이터 은닉

에코 데이터 은닉 방법은 에코의 삽입에 의해 원본 데이터에 데이터를 은닉하는 방법이다. 데이터를 초기 진폭, 지연률, 그리고 오프셋의 세 개의 파라메터로 변화를 주어 데이터를 숨기며, 원본과 에코 사이의 오프셋은 두 시그널을 섞는다. 이 방법은 에코의 삽입에 의해 원본 데이터에 데이터를 은닉하는 방법이다. 중요한 것은 인간의 청력이 두 시그널 사이의 차이점을 구분하지 못한다는 것이다. 그리고 에코는 단지 추가된 소리로 들릴 뿐이라는 것이다.

3.4 스테가노그라피 소프트웨어

상용화된 스테가노 그라피 소프트웨어들은 [7]에서 주로 볼 수 있으며, 아직까지는 주로 이미지와 오디오를 주 매개체로 하는 소프트웨어들이 사용되고 있다. 가장 다양한 매개체를 원본으로 사용하는 것으로는 Invisible Secretes v4.0으로 bmp, jpeg, gif, html, wav 등을 사용한다. 그 외 Steganos Security Suite 4 는 이미지 데이터와 사운드 파일을 지원하며, The Third Eye, Courier, Data Slash, Secure Engine 2, CryptArkan, Camera/Shy vo.2.23.1, Cameleon Stegdetect 등이 있다. 이러한 소프트웨어들을 이용하여 정보은닉을 할 수 있고 재미있는 결과도 경험 할 수 있다.

4. DRM과 디지털 워터마킹

DRM(Digital Rights Management) 기술은 디지털 컨텐츠 유통에 안전성, 유통성, 재사용을 지원하며, 저작권자, 유통업자, 소비자에 이르는 컨텐츠 라이프 사이클에 관계된 모든 에이전트를 만족시켜줄 수 있는 신뢰 구조를 제공하는 기술이다. DRM 자체가 신뢰를 제공하는 비즈니스 모델 구조를 간직하고 있기 때문에 기술이라기보다 모델이나 틀(Framework)이라고 말할 수도 있다

1996년 12월 국제저작권기구인 WIPO (World Intellectual Property Organization; www.wipo.org)는 6년 간 이끌어오던 저작권법을 마무리하면서 3가지 사항을 발표하였는데, 그 중에 1개가 WCT(WIPO

Copyright Treaty)와 WPPT(WIPO Performance and Phonogram Treaty)이며, 본 조항이 디지털 컨텐츠 유통과 관련된 법안인 것이다. WCT와 WPPT의 대표적인 내용은 컨텐츠에 삽입된 권리관리정보(RMI; Rights Management Information)를 보호하는 것으로, 권리관리정보에 기술 조치(Technical Measures)를 취하는 것이고, 본 기술 조치를 파괴하거나, 우회(기술 조치에 쓰여진 정보를 사용하지 않고 컨텐츠를 사용하는 경우), 변경하는 어떠한 소프트웨어나 장치를 제조 또는 판매하는 기관을 처벌하는 것이 주요 내용이다.

DRM 기술의 특징은 Superdistribution(재배포)과 투명한 거래 구조, 그리고 사용 규칙이라는 3가지 특징을 가지고 있다.

재배포는 기존 컨텐츠 유통이 사용자의 공개키로 암호화하고, 사용자의 비밀키로 컨텐츠의 암호화를 푼다면, DRM에서는 컨텐츠마다 키를 생성하여 사용한다. 즉 컨텐츠의 공개키로 암호화하고, 컨텐츠의 비밀키를 판매(또는 허가받은 사람에게 배포)하는 것이다. 그러므로 누구나 허가를 받은 사람은 사용할 수 있는 것이고, 이러한 방식은 컨텐츠를 재활용할 수 있게 하는 것이다. 물론 이러한 방식에는 기본적으로 고려할 사항이 좀더 있다. 즉 어디에서 키를 받을 것인가, 그리고 비밀키는 무한정 유용한가가 의문시 될 수 있으나, 이 또한 간단한 방법으로 해결 방법을 제공하고 있다.

두 번째 투명한 거래 구조는 기본적으로 라이선스를 제공하는 기관과 컨텐츠를 배포하는 기관(쇼핑몰)을 분리함으로써 해결될 수 있다. DRM 환경 하에서 컨텐츠는 반드시 라이선스 파일이 있어야 동작하게 되어있다. 이 라이선스 파일에는 해당 컨텐츠의 비밀키와 사용 규칙 정보 등이 들어있기 때문에 컨텐츠의 암호를 풀기 위하여 라이선스 파일이 필수적인 것이다.

그러므로 컨텐츠 판매의 마지막 단계로 라이선스 제공 기관에 라이선스를 요청하면, 이러한 요청에 대하여 라이선스 제공 기관은 해당 소비자에게 라이선스를 제공하고, 그리고 해당 내역(거래 내역)을 보관하는 것이다. 이것은 일반 상가에서 카드로 물건을 살 경우, 카드로 사용허가를 받는 과정과 동일한 것이다. 이러한 메카니즘은 해당 쇼핑몰이 판매 내역을 감출 수 없으며, 저작권자와 계약을 투명하게 준수할 수 있는 환경을 제공한다. Adobe DRM인 ACS의 경우 또 다른 방법의 투명성을 제공하기도 한다. 즉 컨텐츠 제작시 해당 컨텐츠에 발급할 수 있는 라이선스의 최대량을 고정시키는 것이다. 이 개념은 종이 책 뒷면에 '인지'를 붙이고, 작가가 출판사에게 '인지' 개수를 제어함으로써 책 판매량을 확인하고, 그리고 판매량에 해당하는 로얄티를 받는 구조와 일치한다.

마지막 특징인 사용 규칙(Usage Rules)은 컨텐츠를 소비자가 사용하는데 있어서, 횟수, 날짜수, 장비 환경 등을 통제하는 것이다. 예를 들어 특정 컨텐츠를 '1일 무제한', '1주일에 10번', '1달간 무제한', '1일 1회' 등 볼 수 있는 횟수를 제한하는 것으로, 이러한 횟수에 따라서 해당 컨텐츠의 가격을 차별화 할 수 있기 때문이다. 이때 소비자가 컴퓨터 날짜를 조작함으로써 실제적으로 사용을 연장하려는 시도를 할 수 있는데 이러한 변조를 Tampering이라고 하며, Tamper Resistance 기능이 반드시 DRM에 포함되어야 한다.

지금까지 언급한 3가지 사항이 반드시 있어야만 DRM 제품이라고 할 수 있다. 즉 유통성(컨텐츠의 공개키/비밀키 사용하여 제작), 투명성(저작권자와 유통업자 사이 메카니즘), 사용성(다양한 비즈니스 모델 적용하여)이 보장이되는 것이 DRM 기술인 것이다.

이러한 기술을 뒷받침하기 위해 기반 기술이 되는 것이 디지털 워터마킹이다. 이 기술은 정보은닉의 한 분류로써 숨겨진 정보가 원본에 가해지는 어떤 변형에도 쉽게 바뀌지 않고 정보가 남아 있도록 하는 기술로 저작권이나 묻나 복사 금지 등에 이용되고 있다.

따라서 스테가노그라피에서 설명했던 공격자의 공격에도 강해야 하며 보거나 듣는 것에서도 원본과의 차이가 나타나지 않도록 비밀 메시지(즉, 인증 정보, 사용자 확인, 복사횟수 등)에 관한 정보를 저장하여 DRM 기술에 결합되어 사용되어지고 있다.

5. 결 론

인터넷과 네트워크의 사용이 점점 더 확대되고 사용이 용이해짐에 따라 많은 정보들이 공유되어 사용되어진다. 이러한 정보들은 특별한 제제나 규제없이 사

용되고 있어 디지털 정보 시대에서 윤리나 사회적인 문제가 된다. 따라서 종이로 된 인쇄물 뿐 만아니라 디지털 정보에 대한 권리도 보장받아야 하며, 이를 위해서는 여러 가지 방법과 기술들이 필요하다. 이 연구에서는 디지털 정보에 대한 은닉 기술과 DRM에 대해서 살펴보았으며, 특히 온라인뿐만 아니라 오프라인 상에서 정보 보호를 위한 한 방법으로 많이 사용되는 스테가노그라피 전반에 대해서 설명하였다. 또, 이 기술은 디지털 워터마킹과도 결합되어 멀티미디어 컨텐츠 저작권 관련 기술에 응용되고 있다.

참 고 문 헌

[1] 김현곤, 원동호 외 12, "지적 재산권 보호를 위한 정보 은닉 기술 및 표준화 연구", 한국 전산원, pp.19-41, 2000.

[2] Christian Cauchin, "An Information-Theoretic Model for Steganography", In Proceeding of 2nd Workshop on Information Hiding, Lecture Notes in Computer Science 1525, Springer, 1998, pp306-318.

[3] S.K. Pal, P.K. Saxena, S.K. Muttoo, " The Future of Audio Steganography", STEG'02, July 11-12, 2002.

[4] Neil F. Johnson, "Introduction to steganography Hidden Information", GMU 2001 - Computer Crime Symposium, August 13-17, 2001, George Mason University, Fairfax, Virginia

[5] Fabien A.P. Petitcolas, Ross J. Anderson and Markys G.Kuhn, "Information Hiding - A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062-1078, July 1999.

[6] Stefan Katzenbeisser, and Fabien A.P.Petitcolas "Information hiding techniques for steganography and digital watermarking", Artech House Publishers, 2000

[7] Steganography Software http://members.tripod.com/steganography/stego/software.html

[8] Peter Wayner, "Disappearing cryptography Information Hiding : Steganography & Watermarking", second edition, chapter 17, Morgan Kauffman, 2002.

[9] Bruce Schneier "Applied Cryptography" pp 265-301, 1996

◐ 저 자 소 개 ◑

김 영 실

1989년 고려대학교 컴퓨터학과(이학사)
1991년 고려대학교 컴퓨터학과(이학석사)
1995년 고려대학교 컴퓨터학과 박사과정수료
1998년~현재 : 대림대학 컴퓨터정보계열 조교수
관심분야 : 암호화 및 보안, 멀티미디어와 응용기술

박 성 진

1991년 고려대학교 전산학 (학사)
1993년 고려대학교 일반대학원 전산학 (석사)
1998년 고려대학교 일반대학원 전산학 (박사)
1998년~2000년 한국전자통신연구원 선임연구원
2000년~현재 : 한신대학교 컴퓨터정보통신학부 조교수
관심분야 : XML Respository, Web OLAP & Mining