디지털산업정보학회 논문지 제4권 제2호 - 2008년 6월

프라이버시를 제공하는 저작권 보호 프로토콜

유 혜 정*

Copyright Protection Protocol providing Privacy

Yoo, Hye-Joung

〈Abstract〉

There have been proposed various copyright protection protocols in network-based digital multimedia distribution framework. However, most of conventional copyright protection protocols are focused on the stability of copyright information embedding/extracting and the access control to data suitable for user's authority but overlooked the privacy of copyright owner and user in authentication process of copyright and access information.

In this paper, we propose a solution that builds a privacy-preserving proof of copyright ownership of digital contents in conjunction with keyword search scheme. The appeal of our proposal is three-fold: (1) content providers maintain stable copyright ownership in the distribution of digital contents; (2) the proof process of digital contents ownership is very secure in the view of preserving privacy; (3) the proposed protocol is the copyright protection protocol added by indexing process but is balanced privacy and efficiency concerns for its practical use.

Key Words : Digital Watermark, Keyword Search, Privacy, Copyright Protection

Ⅰ. 서론

최근 인터넷, 전자출판, 컴퓨터 그리고 멀티미디어 관련 기술의 발전으로 문서, 음성, 사진, 비디오 데이터 등의 다양한 매체들이 디지털화 되어 효율적으로 이용 가능하게 되었고, 현대 사회가 점점 멀티미디어 정보화 사회로 발전함에 따라 인터넷과 통신망을 이용한 멀티미디어 데이터의 수요는 증가하고 있다. 이러한 디지털 멀티미디어 데이터 서비스는 이용자로 하여금 편리하고 신속하게 각종 정보를 획득할 수 있도록 지원함으로써 사회·경제적 효과를 극대화하며, 따라서 세계 각국은 앞 다투어 디지털 멀티미디어 데이터 서비스의 조기 확립에 노력하고 있다.

우리나라에서는 모든 사물이 컴퓨터의 역할을 하며 서로 연동하는 새로운 사회의 모델을 제시하는 핵심어인

* 세종사이버대학교 정보보호시스템전공 교수

유비쿼터스 컴퓨팅 기술을 기반으로 국가의 자원을 네트워크상에서 통합하여 삶의 질을 향상시키고 국가 경제 발전을 추구하려는 u-Korea 전략이 정보통신부를 중심으로 추진되고 있다.

'u-Korea'라는 지능기반사회에 진입하기 위해서는 IT 분야의 서비스, 인프라, 기술개발의 3가지 요소가 서로 균형적으로 발전해야 하고 이를 목표로 하는 것이 IT839 전략의 핵심이다.

몇 해 전 우리나라의 국책 선행과제로 출현하게 된 IT839 전략 중 8대 신규서비스에는 정지 및 이동 중에서도 언제 어디서나 고속으로 무선 인터넷 접속이 가능한 휴대인터넷 서비스, 고품질의 음성 및 영상서비스를 언제 어디서나 제공할 수 있는 이동멀티미디어 방송인 DMB(Digital Multimedia Broadcasting) 서비스 그리고 대화면·고화질·입체음향의 고품질 방송을 제공할 수 있는 지상파 DTV 서비스가 포함되어 있으며, 9대 新성장 동력에는 디지털 콘텐츠를 담고 있다.

우리 사회는 무한히 반복 사용하여도 원본의 품질에는 전혀 손상이 없고, 수정과 복사가 편리하며, 초고속 통신망을 이용하여 대용량의 저작물이라도 짧은 시간 안에 전송과 배포가 가능하다라는 디지털의 특성과 장점으로 인해 아날로그 형태로 생산, 보관, 관리되던 도서, 음반, 영화, 방송, 신문 등 일반 상거래의 저작물들을 포함한 문화, 교육, 의료 등 다양한 콘텐츠가 대중화된 관련 IT 기술과 결합하여 디지털화 되고 있으며, 따라서 디지털 형태로 가공처리된 디지털 콘텐츠의 중요성이 증대되고 있다. 이렇듯 디지털 콘텐츠의 중요성이 증대되는 주요 원인은 디지털 콘텐츠 사업이 한계비용 '0'에 가까운 고부가가치 산업으로 이동통신, DTV, 홈 네트워크 등 다른 新성장 동력산업의 부가가치를 증대시키는 핵심 산업이기 때문이다.

그러나 이러한 미래 고부가가치 산업이 결실을 맺기 위해서는 상용화 촉진이 필수적이라 할 수 있다. 특히 디지털 콘텐츠의 유통을 활성화하기 위해서는 개발된 콘텐츠들이 불법복제 되거나 무단배포 되는 것을 방지하고 적법한 사용자만이 콘텐츠를 이용할 수 있는 신뢰성 있는 유통환경을 조성하기 위한 기반기술의 개발과 발전이 반드시 선행되어야만 한다.

콘텐츠의 저작권 침해와 불법복제 등과 같은 문제는 해당 사업의 발전을 저해하는 위험요소가 되고 있으며, 특히, 전자파일 형태로 자유접속이 용이한 인터넷상에서 전송되는 디지털 콘텐츠의 특성 때문에 그 피해 또한 더욱 위협적이라 할 수 있다. 또, 디지털 콘텐츠는 품질의 손상 없이 복제와 변형이 자유롭고 용이하므로 디지털 콘텐츠의 무단복제 및 재배포가 확산되고 있는 실정이며, 이러한 추세에 대응하기 위해서는 디지털 콘텐츠의 소유권 및 지적 재산권을 안전하게 온라인으로 이동시키기 위한 기술개발이 필수적이라 할 수 있다.

여기에서 하나 더 깊이 생각해볼 필요가 있는 것이 개인의 프라이버시 문제이다. 인터넷상에서 이동되는 여러 정보들 중에는 개인의 프라이버시를 침해할 수 있는 여러 가지 개인정보들이 존재한다. 저작권 정보 또한 이러한 개인정보 중 하나라 할 수 있다. 가령 저작권 분쟁이 일어날 경우 현재 시스템 상에서는 저작권자 또는 저작권자가 위임한 저작권 인증 기관(등록 센터 등)이 저작권 정보를 밝혀야만 저작권 권리, 소유 입증이 가능하다. 그러나 저작권 분쟁 해결을 위해 밝혀진 저작권 정보는 다른 사람 소유의 불법적인 디지털 콘텐츠에 이를 삽입함으로써 불법적인 콘텐츠에 대한 차명 유통을 가능하게 해 줄 뿐 아니라, 문제가 발생하지 않고 유통되는 저작권 소유자의 다른 콘텐츠에 대해 정당하게 삽입된 저작권 정보를 제거하는 것을 상당히 용이하게 하여 해당 콘텐츠에서 저작권 정보를 제거한 후 제 3자의 저작권 정보를 삽입함으로써 저작권 증명을 실패하게 할 수 있다. 또한 경우에 따라서 사용자의 온라인 콘텐츠 이용 내역을 추적 가능하게 할 수 있다. 따라서 저작권 정보에 대한 프라이버시 보호는 우리가 지향하는 유비쿼터스 시대에 프라이버시 침해가 매우 심각한 문제로 대두 되는 것과 아울러 반드시 고려되어야 할 사항이다.

저작권을 보호함으로써 콘텐츠의 불법 복제를 막고, 개인의 저작권 정보를 보호함으로써 프라이버시를 제공

할 수 있는 기술을 개발하는 것은 안전하고 건전한 미래 생활을 향유하기 위해 반드시 필요하며, 우리 모두가 원하는 방향으로의 유비쿼터스 사회를 구현하는데 이바지 할 것이라 생각한다.

본 논문에서는 디지털 콘텐츠에서의 개인정보보호 기술을 새로이 제안하고자 한다. 디지털 콘텐츠 유통 상에서 프라이버시 보호적 관점에서의 연구는 디지털 콘텐츠 개발에 있어서 프로토콜적인 새로운 접근이 될 것이고, 더 나아가서 익명성뿐만 아니라 개인 프라이버시 보호에 대한 경각심도 일깨울 수 있다. 그리고 익명성 스킴들이 안고 있는 다소 이론적인 면을 극복하고 디지털 콘텐츠 이동경로 상에서 실질적으로 적용 가능한 프로토콜을 제안하는 계기가 될 것이다.

논문의 구성은 다음과 같다. 제 2장에서는 제안된 프로토콜의 의미와 구조에 관련된 연구들에 대해 간략하게 서술하고, 제 3장에서는 프라이버시를 제공하는 새로운 저작권 프로토콜을 제안한다. 마지막으로 제 4장에서 결론을 끝으로 본 논문을 마무리 짓고자 한다.

Ⅱ. 관련 연구

2.1 저작권 보호 기술

현재 세계 각국에서는 멀티미디어 콘텐츠의 불법복제 및 재배포 방지를 위한 저작권 문제를 해결하기 위한 정보 은닉 기술에 대한 연구가 활발히 진행 중이다. 제시된 해결책으로 기본적인 암호화·복호화 기술 이외에 디지털 워터마킹과 핑거프린팅 등이 있으며, 이 중 암호화와 방화벽을 이용한 접근제어 기술과 디지털 워터마킹 기술이 주로 사용되고 있다[1, 2, 3, 4].

암호를 이용한 기술은 키를 가진 자가 암호 알고리즘을 이용하여 주어진 데이터를 암호화하는 방법으로, 디지털 데이터를 원래의 데이터로 복구하기 위해서는 비밀키를 알고 있어야 한다[5]. 이와 같은 방법은 허가된 권한이 없는 사용자로부터 데이터의 내용을 숨김으로써 콘텐츠에 대한 부적절한 접근을 막는다는 측면에서 사용되고 있으나, 1차적으로 허가된 권한에 의해 내용에 접근한 사용자는 저작권자와 같은 능력을 갖게 되므로 2차, 3차의 불법적인 접근 및 데이터 배포를 막을 수 없다는 문제가 남게 된다. 예를 들어, 케이블 TV나 VOD 시스템에서 요금을 지불한 정당한 사용자만이 비디오를 시청할 수 있으나, 그 이후에 일어날 수 있는 무단복제에 대한 문제는 여전히 남아있게 되는 것이다.

이와 같이 암호는 정보가 전송될 때의 정보보안 이슈를 다루기 위해 일련의 프로토콜과 메커니즘이 수 없이 제안되는 과정에서 아주 긴 역사를 통해 그 안전성이 증명되고 발전되어 왔으나 디지털 콘텐츠의 저작권 보호에 대한 해결책으로는 제한점이 존재하는 것이 사실이다.

디지털 콘텐츠에 대한 안전성을 제공하기 위한 연구로는 고전적인 암호 기법을 사용하여 메시지 자체에 대한 안전성을 확보하고자 하는 연구와 함께 메시지 내에 디지털 정보에 대한 인증 또는 서명에 해당하는 정보를 은닉하고자 하는 연구가 계속되고 있다. 정보은닉 분야는 최근 정보이론에 근간한 스테가노그래피(steganography) 기법과 디지털 워터마킹 기술로 발전하면서 멀티미디어 시대에 저작권 또는 소유권 보호를 위해 필수적인 기술로 부상하고 있다. 이와 더불어 디지털 핑거프린팅 기술을 통해 고전적인 암호 기술을 접목하고 DRM(Digital Right Managements) 기술을 통한 콘텐츠 관리 방식에 대한 연구가 계속 진행되고 있다[6].

스테가노그래피는 기존의 일반적인 암호학 분야와는 다른 목적 및 방향으로 발전한 것으로 전체 메시지에 대한 특성을 유지하면서 정보를 은닉하는 기법이다[7]. 스테가노그래피에서 특히 디지털 정보 및 멀티미디어 콘텐츠에 대한 보호 기법으로 고찰할 수 있는 것이 디지털 워터마킹 기법이다[8]. 디지털 워터마킹 기술은 콘텐츠의 원 소유자를 주장할 수 있는 워터마크 정보를 삽입하여 저작권에 대한 분쟁이 발생할 경우 삽입된 워터마크 정보를 추출하여 저작권을 주장하는 기술이다. 최근 콘텐

츠의 활용 범위 확대와 더불어 워터마킹 기술도 문서의 불법유통 방지, 신분증 위·변조 방지, 디지털 방송, DVD 플레이어, 휴대용 기기 등 다양한 분야로 사용 범위가 확대되고 있다. 디지털 워터마킹 기술은 저작권 정보의 존재성이 주요 성질의 하나이므로 다양한 신호처리 공격 및 고의적인 공격에 대한 강인성과 워터마크 정보의 삽입에 따른 비가시성, 확실한 소유권 증명이 가능하도록 하는 신뢰성 그리고 기본 플랫폼에 대해서 구현 가능한 효율성 등이 요구된다. 디지털 워터마킹 기술은 지적재산권 보호를 위한 기술일 뿐만 아니라 데이터 인증 및 무결성 검증 등과 같은 다양한 분야에 응용 가능하다.

그러나 현재의 디지털 워터마킹 기술은 다양한 방법론이 제시되었음에도 불구하고 많은 한계점을 내포하고 있다. 그 한계점 중 대표적인 것이 디지털 콘텐츠 유통과정에서 저작권 정보 또는 저작권 정보의 부분정보가 노출될 위험이 존재한다는 것과 이로 인한 개인의 프라이버시가 노출될 위험이 존재한다는 것이다. 따라서 본 연구에서는 현재까지 연구가 되어왔던 디지털 워터마킹 기술에 대한 분석을 통해 문제점을 파악하여 기존 워터마킹 기술의 한계점을 극복하고 더불어 디지털 워터마킹 기술에 적합한 프라이버시 보호 방안을 제시하고자 한다.

2.2 데이터 프라이버시

정보화 사회에서 그 정보들의 저장소인 데이터베이스(Database, 이하 DB)의 관리는 무엇보다 중요하며 이를 위한 가장 효과적인 방법은 DB의 암호화이다. 하지만 이에 관한 연구는 주로 이론 중심으로 이루어져 왔으며 따라서 상용화를 위한 보다 효율적이고 현실적인 연구가 활발히 진행되어져야 할 것으로 보인다.

현재까지 암호화하는 방법이 현실성이 없었던 가장 큰 이유로는 암호화된 DB 상에서는 효율적인 자료 검색을 보장 받지 못했다는 것과 암호화된 문서를 검색할 수 있는 사용자가 개인 사용자에게 국한되어 있었다는 것을 들 수 있다. 그러나 이는 새로운 기술 개발을 통해 효율적이고 안전한 자료검색 문제를 해결할 수 있으며, 이는 현재 데이터 프라이버시 관점에서 가장 필요한 기술이라 생각한다[9, 10].

이러한 기술 중 하나로 제시된 것이 바로 암호화된 데이터에 대한 검색 시스템에 관한 연구이다[11, 12]. DB 검색 기술에는 사용자가 원하는 데이터를 미리 만들어 놓고 단순히 이를 꺼내 볼 수 있도록 하는 데이터 웨어하우스(warehouse) 기법과 사용자의 연관된 데이터들의 상관관계를 인공지능 기법을 이용하여 명확히 밝혀서 이를 사용자에게 제공해주는 데이터 마이닝 기술이 있다.

데이터 마이닝은 고정된 자료로부터 알려지지 않았던 중요한 정보를 꺼내어 준다는 의미에서 현실적으로 매우 사용 가치가 높지만, 이로 인해 발생되는 프라이버시에 대한 위협요소 역시 간과할 수 없다. 데이터 마이닝 기술의 기본적인 목적과 방향은 사용자의 프라이버시가 고려되지 않은 채 기술의 정확성을 우선 목적으로 하므로 데이터 마이닝 기술로 파생되는 사용자 프라이버시 문제는 마이닝 기술에 비례하여 발생하는 구조적인 문제를 안고 있다. 따라서 DB에서의 프라이버시 보호 기술은 데이터 마이닝에서의 프라이버시 보호 기술이 주를 이룬다.

이밖에 암호화된 자료를 프라이버시를 보호하면서 어떻게 빨리 검색하느냐에 대한 문제도 큰 이슈로 부각되고 있다[13, 14, 15]. 2000년대에 들어서면서 암호화 기법을 이용한 검색 시스템의 연구가 본격적으로 이루어지기 시작하였으며, 이에 대한 관심의 수준이 매우 높아지고 있다. 특히 D. Song et. al이 제안한 암호화된 데이터를 검색하는 실용적인 기술은 데이터의 기밀성을 잃지 않고 암호화된 정보를 찾을 수 있는 방법을 제공하고 있다[16].

본 논문에서는 암호문이 주어졌을 때 신뢰받지 못하는 서버는 평문에 대한 어떤 정보도 알지 못하는 증명가능한 안전성(provable secrecy)을 가지고 있는 정보 탐색 시스템을 디지털 워터마킹 시스템에 맞게 응용 적용함으로써 암호학적 이론과 정보이론의 관점을 접목, 프라이버시 침해 피해사례를 미리 막지 못하는 저작권 프로토콜의 단점을 극복하고자 한다.

Ⅲ. 프라이버시를 제공하는 저작권 보호 기술

3.1 문제분석(Analysis of Conventional Problems)

저작권 분쟁이 일어날 경우 저작권 소유 주장을 위한 증빙자료로 사용하기 위하여 저작권자나 일반 사용자의 정보를 멀티미디어 데이터에 삽입하는 과정에서 개인정보의 수집·저장은 저작권 보호 콘텐츠 유통 상 필수적인 환경을 구성한다. 저작권 보호 기술 중 다수의 워터마킹 시스템에서는 저작권 분쟁이 발생할 경우 콘텐츠의 유통과정에서 수집·저장된 저작권 정보는 멀티미디어 데이터에서 추출한 정보와 비교하는 과정을 거치게 되며, 이 과정은 콘텐츠에 대한 저작권 증명과 더불어 콘텐츠 인증에도 매우 유용한 방법으로 사용되고 있다.

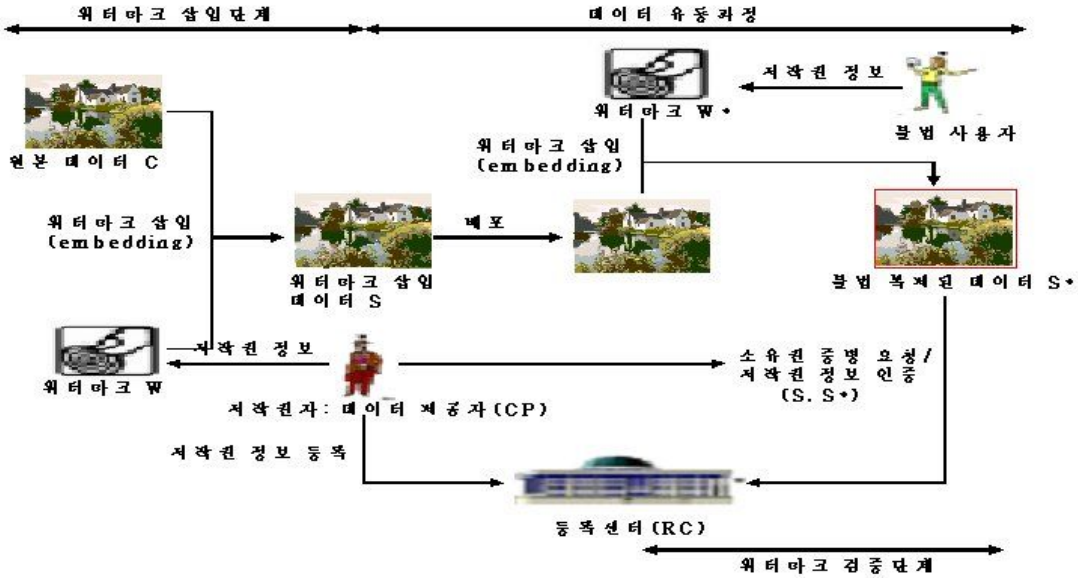
먼저 일반적인 콘텐츠 유통과정과 워터마크 검증 메커니즘은 아래 <그림 1>과 같다. 여기에서 원본 데이터 C와 워터마크 삽입 데이터 S는 가시적인 유사성을 보존해야 하며, 배포된 데이터 S에 불법적인 이용자의 워터마크 W^*을 삽입하여 만들어진 S^* 또한 C 또는 S와 가시적인 유사성을 보존하는 범위에서 변경된 콘텐츠여야만 한다. 따라서 콘텐츠 유통과정에서 생성되는 모든 데이터는 가시적인 부분에서의 유사성을 유지한다는 부분에서 이행성(transitive) 성질을 만족한다고 할 수 있다: $C \sim S$이고 $S \rightarrow S^*$이면, $S^* \sim S$ 또는 $S^* \sim C$

일반적으로 콘텐츠 유통과정에서 저작권 소유자 또는 콘텐츠 제공자(Contents Provider, 이하 CP)가 불법 복제된 콘텐츠를 발견하여 등록 센터(Registration Center, 이하 RC)에 소유권 증명을 요청하는 경우 다음 단계를 거치게 된다.

(1) 저작권 소유자 또는 CP는 RC에 소유권 증명/저작권 정보 인증을 요청한다.

(2-a1) RC는 소유권 증명 요청자에게 저작권 정보를 요청한다.

(2-a2) 소유권 증명 요청자는 저작권 정보를 RC에 전달한다.



<그림1> 콘텐츠 유통과정과 워터마크 검증 메커니즘

또는

(2-b) RC에서는 자신의 저작권 등록 DB에서 소유권 증명 요청자의 저작권 정보를 검색한다.

(3) RC는 소유권 증명 요청자의 저작권 정보와 해당 콘텐츠에서 추출한 저작권 정보를 이용하여 소유권 증명 요청자의 저작권 정보를 인증한다.

(4) 저작권 정보 인증과정이 성공하면 소유권 증명 요청자는 불법 복제된 콘텐츠에 대한 저작권 소유자임을 입증 받을 수 있다.

여기에서 소유권 증명 요청자는 해당 콘텐츠에 대한 저작권 소유자이거나 CP가 되며, CP인 경우 많은 저장 자료 중 해당 콘텐츠의 저작권 정보를 자신의 서버에서 검색하는 과정을 거치게 된다.

기존 디지털 워터마킹 시스템에서는 위 단계를 거치면서

(A) RC에서 소유권 증명 요청자의 저작권 정보를 자신의 저작권 등록 DB에서 찾을 때
(B) 소유권 증명 요청자가 CP인 경우 해당 콘텐츠의 정보를 자신의 저작권 정보 DB에서 찾을 때
(C) 소유권 증명 요청자가 저작권 정보를 RC로 전달할 때
(D) RC에서 저작권 정보를 가지고 인증할 때

의 네 경우에 저작권 정보 유출로 인한 지적재산권에 대한 위협과 더불어 프라이버시 침해 위험이 존재하게 된다. 물론 (C)의 경우 저작권 정보를 암호화하여 전달하는 방법으로 이를 미연에 방지할 수 있으나 그런 경우 소유권 증명 요청자와 RC는 복호화 키를 공유해야 하는 부담을 안고 있다.

대칭 키 암호시스템을 사용하여 복호화 키가 비밀 키인 경우 이는 RC의 신뢰문제로 귀결되며, 공개키 암호시스템을 사용하여 복호화 키가 공개키인 경우 RC에서 관리하고 저장해야 할 데이터의 크기가 커지는 단점을 안고 있다. 또한 저작권 정보를 암호화한다는 것만으로는 (A), (B), 그리고 (D)의 경우 저작권 정보에 대한 부분정보의 유출을 피할 수 없다.

만약 소유권을 증명하는 과정에서 저작권 정보가 유출된다면 저작권 분쟁이 일어나기 전 합법적으로 유통되었던 저작권자의 콘텐츠는 비록 부분 정보만 유출되었다 하더라도 저작권 정보의 불법적인 도용 및 삭제, 프라이버시 침해 등 큰 위험에 처하게 된다. 워터마크에 대한 부분 정보 유출이 저작권 보호 측면에서 얼마나 위험한지는 이미 많은 논문에서 증명되었으므로 본 논문에서는 저작권 정보 삽입 및 유통과정에서 발생되는 위의 (A), (B), (C), 그리고 (D) 네 경우에 대한 저작권 문제와 프라이버시 침해에 대한 해결책을 제시하고자 한다.

3.2 제안기술(Proposed Scheme)

콘텐츠 유통과정에서 저작권과 더불어 프라이버시를 보호하기 위해서는 암호화된 상태에서 저작권 정보를 탐색, 전달, 그리고 인증하는 것이 필수적이라 할 수 있다. 이를 위해서 본 논문에서는 암호화된 저작권 정보로 인증이 가능하도록 함으로써 모든 소유권 증명 과정이 암호화된 상태에서 이루어지도록 하였다.

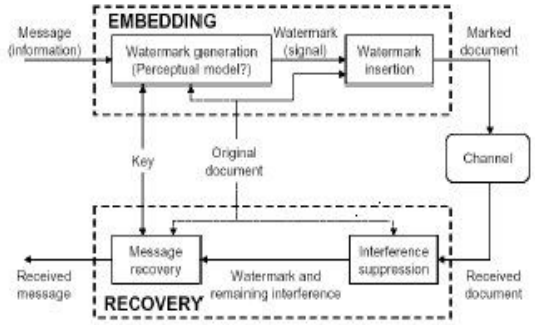
일반적인 워터마크 시스템은 아래 <그림 2>와 같이 크게 워터마크 삽입 단계와 워터마크 추출 단계로 나뉜다.

대부분의 워터마크 시스템에서는 워터마크 삽입단계에서 삽입할 저작권 정보가 콘텐츠의 질을 훼손하지 않도록 하기 위해 워터마크 정보를 눈에 드러나지 않도록 워터마크의 비가시성을 중요시 여긴다. 이를 위해서는 삽입하는 저작권 정보가 기존의 원본 콘텐츠의 정보와 상충하지 않도록 조절하는 것이 필요하다. 즉, 워터마크로 삽입하는 저작권 정보를 정보이론에 근거하여 정보의

균형성을 가지도록 변형하는 과정이 필요한 것이다. 기존 워터마크 시스템에서 이를 위해 주로 사용하는 방법이 바로 저작권 정보의 암호화이다. 따라서 우리가 삽입하고자 하는 저작권 정보를 P라고 하고 워터마크를 W라고 하면, 워터마크 W는 저작권 정보 P가 적당한 암호시스템 E을 통해 나오게 된 암호문이라고 할 수 있으며 ($W=E(P)$), 이 단계가 바로 워터마크 생성 과정이다.

그러나 위에서도 언급했듯이 단순히 암호화 된 워터마크를 사용한다고 하여 프라이버시 침해 문제를 해결할 수는 없다. 본 논문에서는 대칭 키 암호시스템을 사용하여 RC의 저장 데이터가 커지지 않도록 하며, 저작권 증명 과정에서 저작권 정보를 복호화하지 않고 암호화된 데이터를 탐색하여 인증하는 기술을 사용함으로써 저작권자가 RC에 대한 신뢰 문제를 해결하고자 하였다.

본 기술을 사용함으로써 위의 (A), (B), (C) 그리고 (D)의 모든 경우 암호화된 상태에서의 저장, 탐색, 인증을 통하여 저작권 정보 유출과 이로 인한 프라이버시 침해 문제를 해결하게 된다.



<그림 2> 워터마크 삽입 및 추출

먼저 (A) RC에서 요청한 저작권 정보를 자신의 저작권 등록 DB에서 찾을 때와 (B) 소유권 증명 요청자가 자신의 DB에서 저작권 정보를 찾을 때의 안전성을 제공하고자 하는 메커니즘을 설계하도록 한다.

이 문제는 암호화된 자료를 프라이버시를 보호하면서 검색하는 방법을 적용함으로써 해결할 수 있다. 암호화 시스템 E을 통한 암호화는 저작권 정보와 의사난수 비트들의 수열과의 비트별 배타적 논리합을 통해서 간단히 할 수 있는 D.Song et.al[16]에서 제공하는 암호화된 데이터를 검색하는 실용적인 기술을 워터마크 시스템에 맞게 변형하여 적용하였다.

아래 <그림 3>을 기반으로 저작권 정보 생성 및 등록 과정을 설명하면 다음과 같다.

(1) 소유권 증명 요청자는 l개의 의사난수 값 $S_1, S_2, \cdots, S_l$ 수열을 의사난수 생성기 G을 이용하여 생성한다.

(2) 소유권 증명 요청자는 l저작권 정보 $P_1, P_2, \cdots, P_l$을 암호화 한다:

2-1) 키를 가지고 있는 의사난수 함수 F을 선택한다.

2-2) 의사난수 함수 F을 이용하여

$T_i = < S_i, F_{k_i}(S_i) >, 1 \le i \le l$을 계산한다.

2-3) T_i을 이용하여 P_i을 암호화 한다:

$W_i = P_i \oplus T_i$

여기에서 의사난수열 $T_1, T_2, \cdots, T_l$은 소유권 증명 요청자만이 복호할 수 있다.

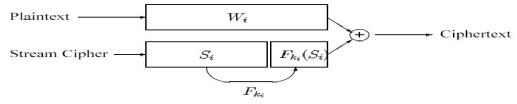
(3) 소유권 증명 요청자는 W_i을 워터마크로 콘텐츠에 삽입한 후 콘텐츠를 유통시키고 이때 소유권 증명 요청자의 DB에는 P_i가 아닌 W_i을 저장하고 RC에도 W_i을 전송한다.

(4) RC는 W_i을 저장한다.

워터마크 삽입단계에서 워터마크를 생성하는 알고리즘은 증명가능한 안전성을 제공하는 탐색을 가능하게 해주므로 (A)와 (B)의 경우 발생할 수 있는 프라이버시 침해 문제를 해결하게 된다. 더불어 소유권 증명 요청자는 RC에 P_i가 아닌 W_i을 전송하여 저작권을 등록하게 되므로 (C)의 경우에 발생할 수 있는 저작권 정보 유출 및 프라이버시 침해 문제를 해결할 수 있게 된다.

워터마킹 시스템에서 인증하는 방법은 아래 <그림 4>와 같이 크게 워터마크 캐스팅 메커니즘(watermark

casting mechanism), 서명 메커니즘(signature signing mechanism), 서명 은닉/증명 메커니즘(signature hiding and verification mechanism)의 세 가지로 구분된다.



<그림 3> 기본 구조(Basic Scheme)

제안하는 워터마킹 시스템에서는 위의 인증 방법 중에서 존재성을 증명하거나 믿을만한(authentic) 워터마크인지를 확인하는 서명 은닉/증명 메커니즘을 사용하며, 이를 위해 C.Cox et.al의 유사 값을 사용하여 저작권 정보의 진위를 결정한다[2].

$$\sim(W_i, W_i^*) = \frac{W_i \bullet W_i^*}{\sqrt{W_i^* \bullet W_i^*}} < \delta$$

여기에서 W_i는 원래의 워터마크를 W_i^*는 콘텐츠에서 추출된 워터마크를 의미한다. W_i는 워터마크 생성과정을 통하여 저작권 정보 P_i을 암호화하여 나온 값이므로 워터마크의 인증과정이 암호화된 정보를 통해서 이루어짐을 알 수 있다. 따라서 위의 (D)의 경우 발생할 수 있는 저작권 및 프라이버시 침해 문제는 해결된다.

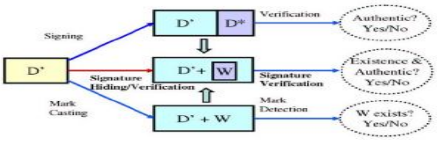
만약 소유권 증명 요청자가 후에 워터마크 정보가 아닌 실 정보를 통하여 자신이 해당 콘텐츠의 저작권자임을 증명하기 원한다면 소유권 증명 요청자는 RC에게 P_i와 P_i의 위치정보를 담고 있는 k_i을 전달하면 된다. 그러면 RC는 암호화된 상태로 저장되어 있는 저작권 정보의 DB에서 $W_i \oplus P_i$가 어떤 S에 대하여 $< S, F_{k_i}(S) >$의 형태인지를 조사하여 P_i가 W_i에 맞는 본 저작권 정보인지를 확인할 수 있게 된다.

위의 프로토콜은 기밀성을 잃지 않고 암호화된 정보로 저작권 정보 탐색이 가능하며, 신뢰받지 못하는 서버는 암호화된 저작권 정보를 통해서는 원래의 저작권 정보를 전혀 알지 못하는, 암호화에 대한 증명 가능한 안전성을 제공받게 된다. 또한 저작권 정보의 생성·삽입단계부터 저작권 분쟁이 발생하는 최종단계까지 모든 디지털 콘텐츠의 유통 과정에서의 저작권 정보 유출로 발생하는 프라이버시 문제를 해결할 수 있게 되는 것이다.

Ⅳ. 결론

본 논문은 디지털 콘텐츠 시장을 활성화하고 국가 미래 정책 과제의 중요한 기반기술인 콘텐츠 저작권 보호 기술을 바탕으로 이미 오랜 세월 검증된 암호기술과 프라이버시 보호 관점에서의 익명성 기술들을 이용하여 저작권 보호 기술을 프로토콜적인 입장에서 새롭게 연구하는 계기가 될 것이며, 디지털 콘텐츠 유통과정에서 유출된 개인정보가 악용되는 것을 막을 수 있는 안전한 프로토콜을 제공하는데 그 의의가 있다고 할 수 있다.

콘텐츠의 불법복제와 프라이버시 침해와 같은 미래 유비쿼터스 사회에 대한 큰 도전을 해결하기 위해서는 법률과 같은 제도적 보완과 더불어 오랜 세월동안 안전성이 증명된 암호기술을 실용화에 초점이 맞추어진 저작권 보호기술에 적용함으로써 안전성과 실용성을 제공하는 기술적 보안이 필수적이라 할 수 있다.



<그림 4> 워터마크 인증과정

매체 중심의 환경에서 콘텐츠 중심의 환경으로 변화하는 현황에 발맞추어 안전하고 편리한 디지털 콘텐츠 보호에 대해서 앞으로 좀 더 깊은 연구를 통해 기술적으로 보완한다면 저작권 보호와 제작자 및 사용자의 프라이버시 보호 기능이 요구되는 관련 응용분야에 많이 활용될 수 있을 것으로 기대한다.

참고문헌

[1] Pfitzmann, B., "Information Hiding Terminology," Information Hiding, Lecture Notes in Computer Science, Springer-Verlag, Vol.1174, 1996, pp. 347-350.

[2] Cox, C., Killian, J., Leighton, T. and Shamoon, T., "Secure spread spectrum communication for multimedia," Technical Report, NEC, Research Institute, 1995.

[3] Boneh, D. and Shaw, J., "Collusion-Secure Fingerprinting for Digital Data," Advances in Cryptology-Crypto 95, Lecture Notes in Computer Science, Springer-Verlag, Vol.963, 1995, pp. 251-263.

[4] Cox, I. J., Killian, J., Leighton, T., and Shamoon, T., "A Secure Robust Watermark for Multimedia," Information Hiding, Lecture Notes in Computer Science, Springer-Verlag, Vol.1174, 1996, pp. 185-206.

[5] Bennett, K., Grothoff, C., Horozov, T., and Patrascu, I., "Efficient sharing of encrypted data," Proceedings of the 7th Australasian Conference on Information Security and Privacy(ACISP), 2002.

[6] Blakely, G. R., Meadows, C., and Purdy, G. B., "Fingerprinting long forgiving messages," Crypto '85, Springer-Verlag, Berlin, 1985.

[7] Craver, S., "On Public-Key Steganography in the Presence of an Active Warden," Proc. of IHW98, Springer-Verlag, 1998, pp. 355-368.

[8] Tirkel, A. Z., Rankin, G. A, Schyndel, R. G., Ho, W. J., Mee, N. R., and Osborne, C. F, "Electronic watermark," Dicta-93, 1993, pp. 666-672.

[9] Chor, B., Gilboa, N., and Naor, M., "Private information retrieval by keywords," manuscript, 1998.

[10] Waters, B., Balfanz, D., Durfee, G., and Smetters, D., "Building an encrypted and searchable audit log," In Proceedings of the 11th Network and Distributed System Security(NDSS) Symposium, 2004, pp. 205-214.

[11] Boneh, D., Crescenzo, G. D., Ostrovsky, R., and Persiano, G., "Public-key encryption with keyword search," Proceedings of Eurocrypt 2004, Lecture Notes in Computer Science, Springer-Verlag, Springer-Verlag, 2004.

[12] E. Go,. "Secure Indexes," A early version of this paper first appeared on the Cryptology ePrint Archive on October 7th 2003, 2004.

[13] Golle, P., Staddon, J., and Waters, B., "Secure Conjunctive Keyword Search Over Encrypted Data," Proc. of the 2004 Applied Cryptography and Network Security Conference, 2004.

[14] Ogata, W. and Kurosawa, K., "Oblivious Keyword Search," Journal of Complexity, Vol.20, 2004, pp. 356 - 371.

[15] Chang, Y. and Mitzenmacher, M., "Privacy preserving keyword searches on remote encrypted data," Cryptology ePrint Archive, Report 2004/05, 2004.

[16] Song, D., Wagner, D., and Perrig, A., "Practical techniques for searches on encrypted data," In Proceedings of IEEE Symposium on Security and Privacy, 2000, pp. 44-55.

■ 저자소개 ■

유 혜 정
Yoo, Hye Joung

2004년 1월~현재
세종사이버대학교
정보보호시스템전공 교수
2003년 3월~2003년 12월
고려대학교 정보보호대학원
연구조교수
2002년 8월 고려대학교 수학과 (이학박사)
1999년 2월 고려대학교 수학과 (이학석사)
1997년 2월 고려대학교 수학과 (이학사)

관심분야 : 디지털 콘텐츠 보안, 암호프로토콜
E-mail : hjyoo@sjcu.ac.kr

논문접수일 : 2008년 5월 18일, 수 정 일 : 2008년 6월 8일(1차)
게재확정일 : 2008년 6월 13일