P2P에서 디지털 콘텐츠 저작권보호를 위한 DRM 시스템 설계

하태진* · 조경옥* · 김종우* · 한승조*
*조선대학교

DRM system design for copyright protection of digital contents in p2p

Tae-Jin Ha*, Kyoung-Ok Cho*, Jong-Woo Kim*, Seung-Jo Han*
*Chosun University
E-mail : ha62@korea.com

본 연구는 산업자원부의 지역현신 인력양성사업의 연구결과로 수행되었음.

요 약

P2P 프로그램은 새로운 e비즈니스 모델의 창출이 무궁무진하다는 평가를 받고 있으나 디지털 콘텐츠 저작권 보호문제가 해결되지 않고 있어 P2P서비스의 발전을 위해서라도 디지털 콘텐츠(digital contents)의 저작권보호 방법에 대한 연구가 시급한 실정이다. 본 논문에서는 인터넷 환경에서 개인 사용자들끼리 디지털 콘텐츠를 주고받을 때 PKI기반의 AES알고리즘을 이용한 디지털 저작권관리(DRM) 기술을 이용해서 보안기능을 제공해주는 P2P시스템을 설계하였다.

ABSTRACT

It is evaluated that there is infinit capability of creating new e business using P2P program. but the research for the method to protect the copyright of digital contents is urgent even for development of the p2p service because the problem of copyright protection for digital contents is not solved. In this article, we designed the P2P system which can give the function of security with technology for copyright management which is made with AES algorism based on PKI when users send digital contants to each other in internet. .

키워드
P2P, 저작권보호, DRM

Ⅰ. 서 론

P2P(Peer-to-Peer)는 현재 활발히 진행되고 있는 인터넷 비즈니스의 중요한 변화를 표현하는 함축적 용어라는 의미를 가진다. P2P서비스는 인터넷 상의 정보를 검색엔진을 거쳐 찾아야 하는 기존 방식과 달리 인터넷에 연결된 모든 개인 컴퓨터로부터 직접 정보를 제공받고 검색은 물론 내려 받기까지 할 수 있는 서비스이다. 이는 웹 사이트에 한정돼 있던 정보추출 경로를 개인이나 회사가 운영하는 데이터베이스로까지 확대할 수 있다. 즉 자신의 정보를 전국적 혹은 세계적으로 관리 운영하며, 회원 상호 간의 다양한 정보 공유뿐만 아니라 동일한 정보를 공유하고자 하는 회원간의 커뮤니티 형성이 가능하며, 그룹웨어로서 역할을 통해 원격회의, 원격교육 등이 가능하다는 것이다. P2P기술이 인터넷에 연결되어 있는 모든 컴퓨터를 네트워크화 시킴으로써 방대한 콘텐츠 저장창고 역할을 하는 반면 그것은 역으로 그 만큼의 저작권 침해의 문제를 안고 있다. 이에 따라 많은 콘텐츠 저작권자들이 P2P 솔루션을 기반으로 하는 온라인 서비스업체를 상대로 저작권 소송을 벌이고 있다. PC통신이나 http를 기반으로 하는 서비스 제공자의 경우 중앙에서 서버를 관리하고 통제함으로써 저작권 위반가능성이 있는 파일들에 대해 제재와 통제가 가능하지만 P2P는 중앙관리체제가 있다고 할지라도 현재의 기술로는 개개인의 파일들에 대한 통제가 용이하지 않다. 또한 저작권문제 이전에 개개인의 컴퓨터를 통제하는 데서 오는 프라이버시 침해 문제 등의 유발가능성이 있어 저작권관리는 쉽지 않을 전망이다. 그러나 P2P가 미래의 비즈니스 모델로서 기대됨에 따라 바이러스와 해킹 등의 보안문제와 함께 저작권문제는 필연적으로 해결해야

할 사안이다.

II. DRM 관련기술

일반적으로 DRM시스템은 다양한 기술들이 조합되어 이루어지는 개념이며 "저작권 관리기술"과 "저작권 보호기술"로 구분할 수 있다.

2-1 저작권 관리기술

저작권 관리기술은 세계적으로 통일된 일련의 관리체계를 마련하기 이한 것으로, 크게 식별(identification), 기술(description) 및 관련 규칙을 설정(rules-setting)하는 기능으로 구분할 수 있다.

- 식별 : 디지털 권한을 효율적으로 집행하기 위한 선행조건으로 책의 ISBN, 음악의 ISWC, 레코딩의 ISRC, 책을 제외한 간행물에 대한 ISSN, 지역 및 국가로 ISO 3166 ISTC등처럼 창작물의 형태에 따라 유일하게 식별할 수 있는 고유번호를 말하며 현재 컨텐츠에 대한 식별체계로서 IDF(International DOI Foundation)에 의해 추진되고 있는 DOI(Digital Object Identifier)라는 표준화 작업이 있다.
- 기술 : 저작권정보가 식별된 뒤 저작자 정보, 저작권자 정보, 출판 날짜, 출판 장소 등과 같은 저작권에 관한 정보를 포함하고 있는 컨텐츠의 메타데이터(meta-data)를 정의한다. 현재 유럽을 중심으로 한 저작권 단체들의 표준화 작업으로는 INDECS(Interoperability of Data in ECommerce Systems)가 있으며 DOI를 지원한다.
- 규칙설정 : 저작자가 컨텐츠에 대한 권한규칙을 설정하는데 사용되는 권리명세언어를 의미한다. 이러한 컴퓨터 기반의 언어는 저작권자가 자신의 지적 재산을 사용자와 상호작용할 수 있도록 매개변수를 설정할 수 있다. 대표적인 권리명세 언어로는 Content Guard의 XrML로 현재 W3C, MPEG21등의 주요 표준 단체에 의해 표준화되고 있다.

2-2 저작권 보호기술

저작권자 및 컨텐츠 제공자는 저작권 보호를 위해 컨텐츠를 허가되지 않은 사용자로부터 안전하게 보호되어야 한다. 저작권 보호를 위한 기술은 암호화 기술을 중심으로 발전되어왔으나, 그 이외에도 디지털 워터마킹 기술, 접근제어 기술 등의 다양한 기술들이 이용되고 있다.

2-2-1. 암호화

암호키는 수학적인 함수를 이용하여 평문을 알아보기 힘든 암호문의 형태로 변환시키는 것으로 안전하게 구현된 암호시스템에서는 키를 알지못하는 사람은 암호화된 데이터를 복호화할 수 없는 기능을 말한다. 예를 들어, 암호화 키와 복호화 키가 같은 대칭키 암호로는 DES, SEED, AES 등이 있으며, 암호화 키와 복호화 키가 다른 공개키 암호로는 RSA, ElGamal 등이 있다. DRM 기술은 암호화된 컨텐츠를 배포하고 복호화 키가 없는 사람은 암호화 된 컨텐츠를 사용할 수 없도록 하고 있다.

2-2-2. 디지털 워터마킹

저작권을 보호하기 위하여 디지털 데이터와 분리할 수 없도록 저작권 정보를 데이터 내에 숨겨둔 후 암호화하여 사용자에게 전송한다. 이때 불법적으로 2차 배포된 디지털 데이터로부터 저작권 정보를 추출함으로써 자신의 저작물임을 증명함과 동시에 저작권 정보에 사용자 정보를 포함시키는 경우에 누가 불법적으로 배포하였는가도 함께 지적할 수 있다. 이것은 디지털 데이터의 암호화만으로는 저작권 보호가 미흡하기 때문에 보완책으로 이용하는 것으로 어떤 디지털 데이터 내에 2차적인 데이터를 몰래 숨겨 놓는 경우를 심층암호(steganography)라 하며 그림과 같이 데이터 은닉(data hiding, data embedding) 기법과 저작권 보호를 위한 기법으로 나눌 수 있고, 후자는 다시 디지털 워터마킹(digital watermarking)과 fingerprinting으로 분류되지만 저작권 보호를 위한 기법을 통칭 디지털 워터마킹이라 한다. 데이터 은닉 기법의 목적은 제3자가 알아차릴 수 없도록 비밀 데이터를 다른 데이터에 몰래 숨겨서 전송하기 위한 것이기 때문에 이 기법은 비밀 데이터의 존재 여부의 검출(detection)에 대하여 견고하게 숨길 수 있도록 설계되어야 한다. 데이터 은닉 기법은 영상, 오디오, 비디오와 같은 데이터뿐만이 아니라 네트워크 상의 패킷과 같은 일시적으로 발생하는 데이터들 내에 비밀 데이터를 숨겨두는 경우도 포함하고 있다. 이러한 데이터 은닉 기법을 기반으로 디지털 워터마킹은 워터마크(watermark)라는 저작권 정보를 디지털 데이터 내에 숨겨 두어 저작권을 보호하고자 하는 특수한 목적으로 이용한다.

III. 제안된 P2P내의 DRM 시스템 설계

본 연구에서는 P2P 시장이 확대와 유료화를 전환되면서 발생되고 있는 저작권문제와, 해킹 바이러스에 대한 P2P 프로그램의 보안, 컨텐츠 보호, 불법 자료, 지불에 대한 인증 등의 문제점들을 해결하지 위한 P2P 시스템을 개발하고자 한다. 본 논문에서 연구되어야할 기법으로는 다음과 같다.

- 인증서를 이용한 전자서명 생성 및 검증, 암/복호화
- 불법 컨텐츠 배포의 부인 방지
- 저작권 자동 지불 시스템
- PKI기반의 권한정보 처리 기법 활용으로 위변조 방지
- 컨텐츠의 사용권한 제한 : 읽기 회수 및 사용기간 제어, 인쇄 제어, 문서 전달 제어
- 설정된 사용 권한이 종료되면 자동 파기

- Copy & Paste 방지, Drag & Drop 방지, 화면 캡쳐 방지, 저장 방지 등
- 저작권 파일 워터마킹을 이용한 자동인지 및 지불 시스템

3-1 사용자 신뢰성과 인증 문제

P2P 시스템에서 End-User 사이에서 허위사용자나 신뢰할 수 있는 사용자인지를 확인하고 자신의 신분을 증명할 수 있는 시스템 개발하고자 한다. 이러한 기능은 허가 받지 않은 사용자의 접속이나 위장접속의 문제를 해결할 수 있는 기능이다.

이러한 문제를 해결하기 위해서 Peer to Peer 접속시 PKI를 이용하여 신분을 확인토록 하는 프로그램을 개발한다. PKI를 이용하여 상대방의 인증을 함으로써 신뢰성 있는 콘텐츠 공유를 할 수 있다.

i. P2P 메인 서버에서는 사용자들에게 가입시 각각의 공개키(KUa, KUb)와 개인키(KRa, KRb)를 분배한다.

ii. 상대방의 컴퓨터에 접속시 자신의 개인키로 암호화(E)된 접속정보와 개인인증 정보(IA, IB)를 교환한다.

$$Peer\ A \Rightarrow Peer\ B : E_{KUa}(I_A)$$

$$Peer\ B \Rightarrow Peer\ A : E_{KUb}(I_B)$$

iii. 이러한 정보를 각 상대방의 공개키를 이용하여 복호화(D)하여 상대방 인증 및 확인을 한다.

$$Peer\ A : D_{KRa}[E_{KUa}(I_A)]$$

$$Peer\ B : D_{KRb}[E_{KUb}(I_B)]$$

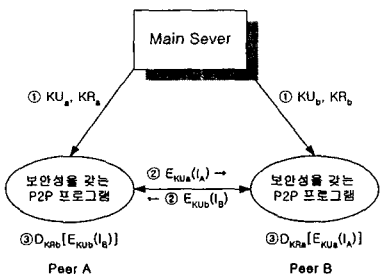

그림 5 사용자 인증을 위한 보안 P2P 시스템

3-2 불법 컨텐츠 배포의 부인방지

많은 불법 자료들이 P2P를 통하여 배포되고 있다. 이러한 문제는 법적으로도 문제가 있는 만큼 불법 자료 배포자에 대한 증거를 확보할 수 있는 기능이 제공되어야 한다.

i. Peer B가 Peer A에게 다운로드 요청을 하면,

ii. P2P 시스템에서 A의 개인정보(IA)와 컨텐츠 정보(C)를 해쉬함수(H)를 이용하여 메시지다이제스트(MDA)를 Server에 전송한다.

$$MD_A = H(I_A \parallel C)$$

iii. 컨텐츠의 다운로드를 Peer A에서 Peer B로 시작한다.

iv. 다운로드가 완료되면 B측에서 자신의 개인정보(IB)와 컨텐츠 정보(C)를 해쉬함수(H)를 이용하여 메시지다이제스트(MDB)를 Sever에 전송한다.

$$MD_B = H(I_B \parallel C)$$

v. Sever는 MDA와 MDB를 로그파일로 저장한다.

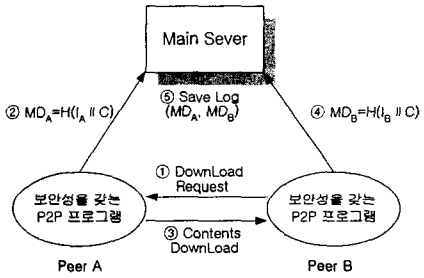

그림 6 불법컨텐츠 배포 부인방지를 위한 보안 P2P 시스템

3-3 저작권 해결 문제

현재 저작권 컨텐츠 자료를 P2P를 이용한 불법 유통으로 인하여 사회적 물의를 일으키고 있다. P2P 시장이 커짐에 따라 이러한 불법 행위의 단속은 점점 힘들어 지고 있다. 또한 현재의 P2P 구조상 저작권료 지불에 대한 뚜렷하고, 안전한 방법이 없다.

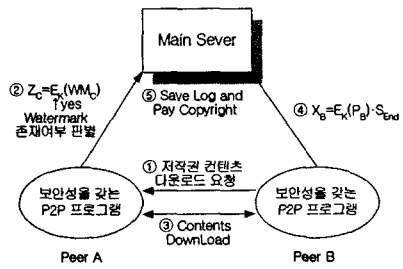

그림 7 저작권료 자동 지불 보안 P2P 시스템

본 연구에서는 저작권 표시가 있는, 즉 저작권의 Watermark가 삽입되어 있는 컨텐츠의 경우 P2P 시스템이 자동으로 인지하여 Watermark정보(WM_C)를 암호화($Z_C=E_K(WM_C)$)하여 Server에 자동 전송함으로써, 다운로드 완료 신호(S_{End})와 함께 저작권료를 자동 지불할 수 있다. 이러한 시스템은 저작권료에 대한 자동 데이터 베이스와 자동 지불이 가능하다.

3-4 불법 다운로드 및 고의적 접속 차단자의 해결

E-DES 알고리즘을 이용하여 디지털 콘텐츠를 보호한다. 데이터 전송시 E-DES 알고리즘을 이용하여 암호화($Y=E_{KUb}(C)$)한 후, 완료시 마지막에 B의 공개키를 이용하여 키값을 전송하는 구조로 설계한다. 이러한 방법은 고의적인 접속 차단자뿐만 아니라, 불법적인 도청 및 해킹을 방지할 수 있다.

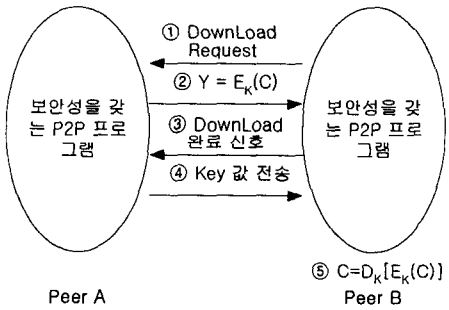

그림 8 불법 다운로드 및 고의적 접속 차단을 위한 보안 P2P 시스템

3-5 불법 복사 방지 및 불법 배포 등 실행 제한 기능

위와 3-3과 같은 방법을 이용하여 저작권 문제를 해결한다고 해도, 다운로드받은 사용자가 임의로 복사나 배포, 컨텐츠의 불법 사용하는데는 대비책이 없었다.

본 연구에서는 컨텐츠의 복사나 배포, 불법 사용에 제한을 가할 수 있는 기능을 추가한다. 컨텐츠에 제한적 사용 옵션이 설정되어 있는 경우, P2P 시스템이 사용자 컴퓨터의 고유 정보(예, HDD의 코드번호, CPU 고유번호 등)를 이용하여 킷값을 생성 암호화하여 저장한다. 제한 옵션이 설정되어 있는 컨텐츠의 경우 실행을 위해서는 반드시 P2P 프로그램을 이용하여 복호화하여 실행되게 한다. 이러한 컨텐츠는 만약 본인이 사용하여 제한된 사항을 전부 소진하였다 하여 쓸모 없게 되더라도, P2P 시스템을 이용하여 타인에게 배포할 수 있다. 제한 옵션에는 '몇 번만 실행', '몇 번 복사 가능', '복사 불가', 등의 정보가 들어 있다.

제한 옵션이 설정되어 있는 컨텐츠가 전송될 때는 다음과 같다.

i. 송신측 P2P 시스템에서는 암호화한 킷값(K_{ia})을 이용하여 실행제한 옵션 설정이 되어 있는 컨텐츠($E_{Kia}(C_a)$)를 복호화 ($C=D_{Kia}[E_{kia}(C_a)]$)한다.
ii. 컨텐츠(C)의 옵션값을 리셋($Rs(C)$)하여 다시 암호화($Y=E_K(Rs(C))$)하여 전송한다.
iii. 수신측 P2P 시스템에서는 수신측의 컴퓨터 정보를 이용하여 킷값(K_{ib})을 생성하여 컨텐츠를 암호화($C_b=E_{Kib}(C)$)하여 저장한다.
iv. 컨텐츠의 실행을 위해서는 P2P 시스템을 이용하여 실시간 복호화하여 실행 ($C=D_{Kib}[E_{Kib}(C)]$)한다.
v. 실행 완료 후, 컨텐츠의 정보를 갱신(C_{-1})하여 암호화($C_{b-1}=E_{Kib}(C_{-1})$)한다.

이러한 방법은 컨텐츠 자체를 암호화하여 저장하고, P2P 시스템을 이용하여 실행하기 때문에 복사, 불법 배포 및 크랙에 안전하다.

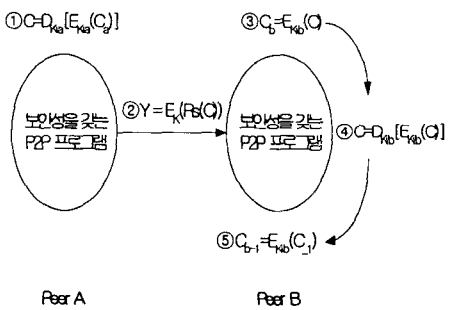

그림 9 불법 복사 방지 및 실행제한 기능을 갖는 보안 P2P 시스템

IV. 결 론

P2P는 무한대의 디지털 콘텐츠 공유, 서버의 부하와 트래픽 감소, 사용의 편리성 등의 장점 때문에 급속한 성장을 하고 있다. 이러한 P2P는 지금까지는 많은 업체에서 무료로 서비스를 제공하였으며, 현 시점에서 유료화로의 변환이 계속되고 있다. 과거에는 많은 업체들이 무료로 서비스를 제공해왔기 때문에 트래픽과 서버부하의 문제점 해결을 중점적으로 해결해왔다. 그러나 정보의 사회가 발달되고 디지털 컨텐츠시장이 커짐으로써 보안이라는 개념이 중요시되고 있다. P2P 서비스에서 보안의 개념이 접목이 되지 않는다면, P2P 서비스의 성장은 한계에 부딪힐 것이다. 본 논문에서는 디지털 콘텐츠 공유를 위한 통합 P2P 시스템을 개발함으로써 P2P 시장의 안정적인 성장에 이바지할 수 있다.

본 논문을 통하여 안전한 결제구조를 통한 자금흐름 유도, 사용자 인증과 컨텐츠의 암호화를 이용하여 신뢰성 있는 컨텐츠의 공유를 유도할 수 있고 컨텐츠의 저작권료를 해결함으로써 창작물에 대한

보호와 저작권료에 관련한 분쟁을 해소할 수 있다. 저작권료 문제가 해결됨으로써 디지털 컨텐츠 창작문화에 활력소를 불어넣을 수 있다 이는 다시 P2P 시장의 발전으로 환원되어 P2P 프로토콜은 차세대 네트워크의 중요한 프로토콜로 성장할 것이다. 본 논문에서 DRM기술은 P2P뿐만 아니라 나아가 온라인을 통한 디지털 콘텐츠 판매 사업에 활용될 수 있다.

참고문헌

[1] S. J. Han, H. S. Oh, "Design of Extended-DES cryptography," Proc- eeding of the IEEE International Symposium on Information Theory, pp.353-359, July 1995.

[2] S. J. Han, "The Improvement Data Encryption Standard(DES) Algorith- m," Proceedings of ISSSTA '96, IEEE, pp.1167-1171, Sept. 1996.

[3] S. J. Han, "Improved-DES Crypto- system Design." Journal of Kiss, Vol.24, no.1, pp.57-67, Jan. 1997.

[4] Uecision Diffie-Hellman, and Discrete Logarithms," ISIT 1998, Cambrige, MA, USA, August 21-26

[5] http://www.openp2p.com/

[6] http://www.jxta.org/

[7] Matei Ripeanu, "Peer-to-Peer Architecture Case Study: Gnutella Network", techreports TR-2001-26, University of Chicago, July, 2001.

[8] C. K, Cok, High-Speed RSA Implementation, TR 201, November 1994.

[9] "전자 서명 인증서 프로파일 표준", TTAS. KO-12. 0012. 한국정보통신기술협회, 2000.12

[10] PKI forum White Paper. "CA-CA Interoperability." PKI forum. 2001.3

[11] Government of Canada Public-Key Infrastructure Cross-Certification Methodology and Criteria. Draft Version dated April 2000