

# 실행시간과 안전성을 고려한 웹 기반의 저작권관리 시스템

고 일 석\* · 조 용 환\*\* · 신 승 수\*\*\* · 조 도 은\*\*\* · 권 영 애\*\*\*

## 요 약

디지털콘텐츠는 복제가 용이하고 원본과 복사본이 동일하다는 특성 때문에 불법적인 복제와 유통의 방지를 통한 저작권의 보호에 어려움이 있다. 근래에는 웹을 기반으로 한 각종 디지털콘텐츠 서비스 시스템이 상용화되고 있으며, 이것이 안정된 수익 모델로서 발전하기 위하여 적절한 저작권 보호 기술이 요구된다. 일반적으로 웹 기반의 저작권 보호를 위해서는 디지털콘텐츠의 암호화를 통한 안전한 전송 방법을 사용한다. 이때 암호화된 디지털콘텐츠의 크기는 증가하여 실행과정에 필요한 시간을 증가시킨다. 따라서 실행시간과 안전성을 고려한 시스템의 설계가 필요하다. 본 연구에서는, 디지털콘텐츠의 저작권 관리 기술을 기반으로 부분 암호화를 통해 수행시간과 안전성을 고려한 디지털콘텐츠 전송 시스템을 설계하였다. 또한 분석을 통해 제안시스템의 성능을 평가하였다.

## A Web-based Right Management System Considering Execution time and Security

Il-Seok Ko\* · Yong-Hwan Cho\*\* · Seung-Soo Shin\*\*\*  
Do-Eun Cho\*\*\* · Yong-Ai Kwon\*\*\*

## ABSTRACT

As for the digital content, a reproduction is easy and manuscript is identical with original copy. Because of these characteristics, there are difficulties on prevention of an illegal reproduction and an illegal currency. In recent days various digital content service systems based on a web are commercialized. An appropriate copyright protection technology is required so that these systems develop as a profit model. Generally we use encrypted digital content transmission method for the copyright protection on a web base system. At the time of this, it is increased size of encrypted digital content. As for this, it be increased time required on an execution process. Therefore, a design of the system that considered a execution time and a security is required. In this study, we designed the digital content transmission system that considered execution time and a security through a partial encryption based on a digital content copyright management technique. Also we evaluated performance of a proposed system through analysis.

**키워드** : 저작권보호(Copyright Protection), 디지털콘텐츠(Digital Content), 부분암호화(Partial Encryption)

### 1. 서 론

정보통신 산업의 발달로 네트워크의 속도가 향상되었고 디지털콘텐츠의 웹을 통한 유통이 확산되고 있다[1]. 웹을 이용한 디지털콘텐츠의 유통은 저렴한 유통 비용 절감과 Try-Before-You-Buy, Pay-Per-Use 등의 다양한 방법의 구매가 가능한 장점이 있다. 하지만, 디지털콘텐츠는 복제의 용이성으로 인해 저작권 보호와 불법복제/유통 방지에 어려움을 겪고 있는 실정이다. 또한 불법복제된 디지털 정보의 발견 및 불법복제 여부의 기술적인 판단과, 이를 법적으로

보호받기 위한 최종 과정인 재판을 통한 판결과 배상까지 시간과 노력의 투자가 힘든 실정이다. 따라서 저작권을 보호하고 고객의 다양한 욕구를 만족시키며 콘텐츠 산업을 활성화시킬 수 있는 진보된 콘텐츠 제공 시스템 구축을 위한 기술 개발이 필요한 실정이다. 또한 일반적으로 웹 기반의 저작권 보호를 위해서는 디지털콘텐츠의 암호화를 통한 안전한 전송 방법을 사용한다. 이때 암호화된 디지털콘텐츠의 크기는 증가하여 실행과정에 필요한 시간을 증가시킨다. 따라서 실행시간과 안전성을 고려한 시스템의 설계가 필요하다.

본 연구에서는, 디지털콘텐츠의 저작권 관리 기술을 기반으로 부분 암호화를 통해 웹 기반의 안전하고 효율적인 디지털콘텐츠 전송 시스템을 설계하고 분석을 통해 성능과

\* 정 회 원 : 충북과학대학 전자상거래과 교수  
 \*\* 정 회 원 : 충북대학교 전기전자컴퓨터공학부 교수  
 \*\*\* 정 회 원 : 충북대학교 대학원 컴퓨터공학과  
 논문접수 : 2003년 5월 12일, 심사완료 : 2003년 10월 28일

안전성을 확인하였다.

### 2. 관련 연구

인터넷에서 웹을 이용하여 클라이언트와 서버사이의 신뢰성과 안전성을 확보하기 위해서는 웹 보안 프로토콜과 평문 데이터를 암호화 및 복호화하는 알고리즘이 필요하다 [2,3]. 웹 보안 프로토콜에는 응용 계층에서 메시지 전체를 암호화하여 전송하는 방식과, 메시지에서 몸체 일부분만을 암호화하여 전송하는 방식이 있다. 또한 SSL과 같이 응용 계층과 전송계층 사이에 암호화 계층을 별도로 삽입하여 암호화하는 방법이 현재 많이 사용되고 있다[4]. 웹클라이언트와 서버 사이의 신뢰성과 안전성을 확보하기 위해서는 클라이언트와 서버 각각을 인증서(CA)를 통하여 인증 받는 절차가 필요하다. 이때 사용되는 데이터의 집합이 인증서이다. 인증서의 형식으로 가장 널리 사용되는 표준은 ITU-T의 X.509이다[5].

미국에서 개발한 DES은 64비트 대칭키 알고리즘이며[6], 현재는 세계 각국에서 IDEA, FEAL, RC-5 등이 개발되어 사용되고 있다. 한국의 경우 SEED라는 128비트 대칭키 알고리즘이 표준으로 제정되어 있다[7].

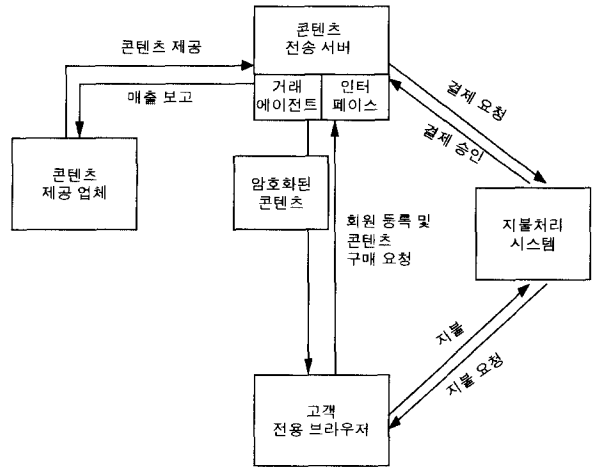
공개키 암호방식은 암호화할 때 사용하는 키(공개키 : public key)와 복호화할 때 사용하는 키(비밀키 : private key)가 달라서 공개키는 공개하고 비밀키만 안전하게 유지하는 방식이다[2,8]. 공개키 기반의 웹 보안 시스템에서는 클라이언트와 웹서버의 인증이 종료된 후에 암호화 채널을 형성하여 실질적으로 데이터를 주고받을 때는 공개키와 비밀키를 이용한다. 공개키 개념이 발표된 후 많은 알고리즘이 발표되었지만, 현재 가장 안전성을 인정받고 있는 것은 RSA와 Diffie-Hellman 알고리즘 등이 있다. 실제로 많은 웹 상용 보안시스템의 경우 RSA 공개키 알고리즘을 이용하고 있다. RSA 방식은 계산에 소요되는 시간이 대칭키 방식에 비해 오래 걸리지만 공개키 방식은 대칭키 방식에 비해 암호화 과정에서 사용하는 키의 안전한 분배가 용이하여 상용 시스템에서 많이 사용되고 있다.

또한, 디지털콘텐츠 전송 모델은 SecuMAX와 Digicap, DLC(Dynamic Licence Control) 기술을 사용한 모델 등이 있으며 이들 모델은 다음과 같은 저작권 관리 기술과 저작권 추적 기술을 사용하고 있다.

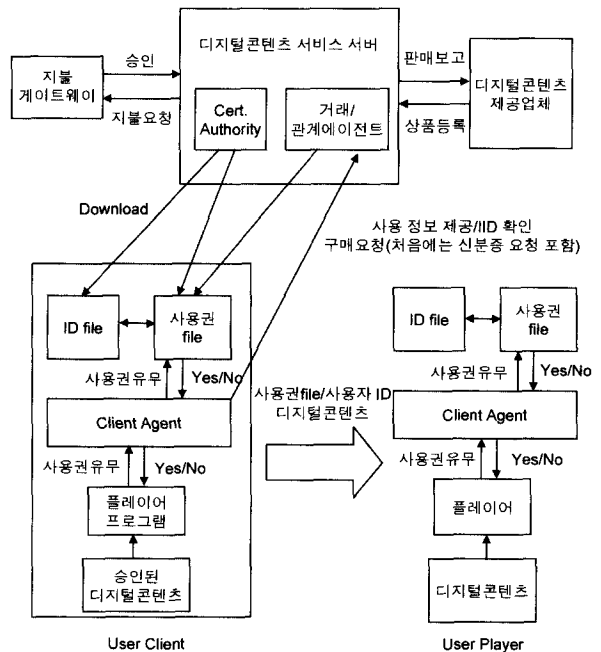
### 3. 시스템 설계

제안시스템은 온라인에서 에이전트를 사용한 디지털콘텐츠 전송시스템이며, 콘텐츠 전송서버, 전용브라우저, 암호화된 콘텐츠와 콘텐츠 제공업체 서버, 지불처리시스템 등으로 구성된다. 제안시스템은 디지털콘텐츠의 저작권 관리를 위

해 필수적인 기능인 암호화 및 키 관리, 전용 브라우저를 통한 디지털콘텐츠의 지속적인 보호 기술이 가능하다. (그림 1)은 시스템의 구성을 나타낸 것이고, (그림 2)는 시스템에서 동적 저작권관리 방법을 나타낸 것이며, (그림 3)은 서버 측 전송 인터페이스를 나타낸 것이다.



(그림 1) 시스템 구성

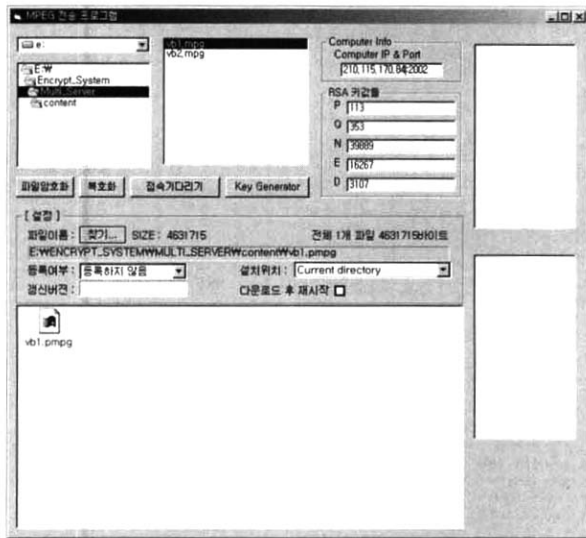


(그림 2) 동적 저작권 관리 방법

서버 측에서 암호화된 동영상 파일을 전송하기 위한 프로그램 운용 과정은 네 부분으로 구분된다. 첫 번째로 전송 인터페이스에서 [Key Generator]를 클릭하여 RSA 암호화 알고리즘에서 사용되는 공개 키 N, E와 비밀 키 P, Q, D의 키 값이 생성한다. 두 번째로 탐색창에서 암호화 할 파일을 선택하고 [파일암호화]를 클릭하여 암호화하여 준다. 세 번째로 [설정] 창에서 [찾기...]를 클릭하여 암호화한 파일을

파일 전송 리스트에 추가를 시킨다. 마지막으로 [접속기다리기]를 클릭하여 클라이언트 측 전용브라우저의 접속을 대기하고, 접속 후 전용브라우저의 다운로드 요청에 의해 암호화된 동영상 파일을 전송하게 된다.

클라이언트 측 전용브라우저는 동영상 파일의 전송과 재생 역할을 한다. 전송을 위해 [Server IP]를 설정(Default IP)하고 [Download]를 클릭하면 서버측의 암호화된 동영상 파일을 요청하여 다운로드 하게 된다. 재생을 위해 [Play]를 클릭하면 다운로드 받은 동영상 파일이 복호화 과정을 거쳐 재생된다. 복호화 과정은 서버 측 암호화 과정의 역과정으로 수행된다.



(그림 3) 서버 측 전송 인터페이스

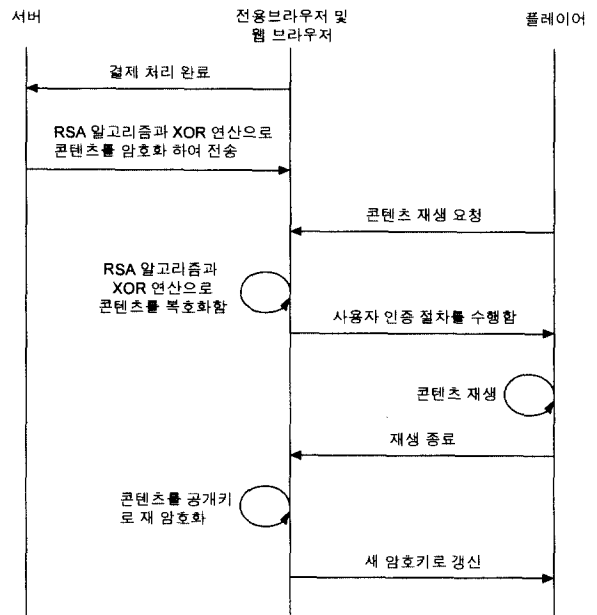
콘텐츠 제공 업체는 콘텐츠 판매자에게 콘텐츠를 제공하고 판매 보고를 받는다. 콘텐츠 전송 서버는 콘텐츠 제공 업체로부터 제공받은 콘텐츠로부터 샘플 콘텐츠와 판매자의 대칭키로 암호화된 콘텐츠를 갖추게 된다. 판매와 회원 관리는 거래 에이전트가 처리하게 된다. 고객은 등록을 하고 전용 브라우저를 자신의 컴퓨터에 전송 받아 설치하게 한다. 고객의 콘텐츠 구매 요청이 들어오면 지불 처리 시스템에게 결제를 의뢰하며 결제승인이 되면 해당 콘텐츠를 전송하고 판매 상황을 업체에 통보한다. 지불처리 시스템은 콘텐츠 전송 서버로부터 결제 요청에 대해 해당 고객에게 지불을 요청하며 지불이 완료되면 서버에게 결제를 승인한다. 구매자는 서버에 접속하여 회원 등록을 하고 전용 브라우저를 전송 받아 설치한다. 검색과 샘플 콘텐츠를 이용하여 원하는 콘텐츠를 선택한다. 지불 과정을 마친 후 전용 브라우저를 통해 콘텐츠를 전송 받아 재생한다.

사용자의 구매 요청에 대해 콘텐츠는 대칭키를 이용하여 암호화되며 전송 시 다시 공개키로 암호화하여 전송한다. 사용자가 전송 받은 콘텐츠를 재생하기 위해 전용 브라우

저에 내장되어 있는 플레이어의 재생 버튼을 클릭하면 전용 브라우저가 개인키와 대칭키를 이용하여 복호화 한다. 재생이 종료되면 전용 브라우저가 즉시 콘텐츠를 공개키로 암호화하여 콘텐츠를 암호화 상태로 관리하게 된다. 사용자는 새로운 개인키를 부여받는다.

### 3.1 콘텐츠 암호/복호화 과정

사용자가 콘텐츠를 요청 할 경우 RSA 암호화 알고리즘과 XOR 연산을 수행하여 암호화한 콘텐츠를 전송한다. 사용시스템을 기반으로 할 경우, 전체콘텐츠를 암호화하면 사이즈의 엄청난 증가를 가져와 결국 실행 시간을 떨어뜨리는 요인이 된다. 따라서 부분암호화를 통하여 처리하며, 암호화와 복호화에 거의 시간적으로 영향을 주지 않기 위해서 암호화하지 않은 부분에 대해서 XOR 처리를 한 것이다. 결국 실행시간과 암호화 강도의 트레이드 오프가 발생하게 된다. 또한 재생 완료 즉시 전용 브라우저로 암호키를 갱신함으로써 콘텐츠와 전용 브라우저를 1:1 관계로 묶어 저작권을 보호한다. 콘텐츠의 암호화 및 복호화 수행 과정은 (그림 4)와 같다.



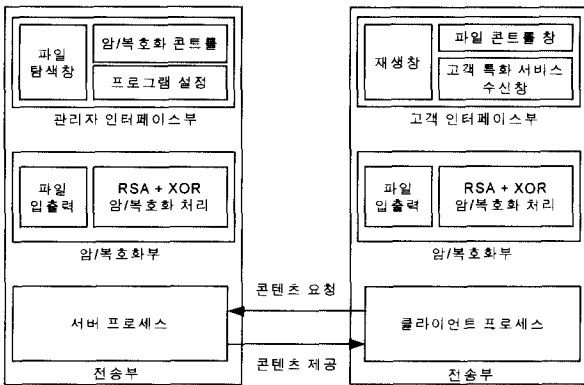
(그림 4) 콘텐츠 암호화/복호화 수행 과정

사용자로부터 구매 요청을 받으면 RSA 암호화 알고리즘과 XOR 연산을 사용하여 콘텐츠를 암호화한다. 사용자가 전송 받은 데이터를 재생하기 위해 플레이어의 재생 버튼을 클릭한다. 다음으로 전용 브라우저가 RSA 암호화 알고리즘과 XOR 연산을 사용하여 콘텐츠를 복호화한 후, 전용 브라우저가 사용자 인증 절차를 수행한다. 그리고 플레이어가 콘텐츠를 재생하게 된다. 이제 재생을 종료한 후 전용 브라우저가 콘텐츠 재암호화하고 사용자 키를 갱신한다.

3.2 전용 브라우저

제안시스템은 전용브라우저를 통해 암호화된 콘텐츠의 전송 및 서비스가 가능하다. 따라서 전용브라우저의 기능은 제안시스템의 성능에 많은 영향을 미친다. 전용 브라우저의 요구 사항은 다음과 같다.

- ① 시스템 서버의 콘텐츠를 열람할 수 있는 기능
- ② 사용자 개인 정보 송신과 디지털콘텐츠의 수신 기능
- ③ 디지털콘텐츠의 암호화/복호화 기능
- ④ 플레이어와 유기적 관계 형성
- ⑤ 콘텐츠 재생 시 서버와의 연결을 통해 동적인 정식 사용자 확인 기능
- ⑥ 콘텐츠 재생시 동일 네트워크 상의 동시 사용 여부 체크 기능



(그림 5) 전용 브라우저의 구성

전용 브라우저는 서버 측의 암호화 프로그램과 클라이언트 서버의 관계를 갖는다. 그러므로 전용 브라우저를 설계하기 위해서는 서버 측의 암호화 프로그램을 고려해야 한다. 또한 서버 측 암호화 프로그램은 크게 관리자 인터페이스부, 암/복호화부, 전송부로 나누어 볼 수 있다. 관리자 인터페이스부는 파일 탐색창, 암/복호화 콘트롤, 프로그램 설정 등을 제공한다. 암/복호화부는 RSA 알고리즘과 XOR 연산을 이용하여 콘텐츠를 암/복호화한다. 전송부는 서버 프로세스를 담당한다. 그리고 전용 브라우저는 크게 고객 인터페이스부, 암/복호화부, 전송부로 나누어 볼 수 있다. 고객 인터페이스부는 파일 컨트롤창, 콘텐츠 파일 재생, 고객 특화 서비스 수신창 등으로 구성된다. 암/복호화부는 콘텐츠 재생 전에 파일을 복호화하고 재생이 끝나면 암호화를 한다. 전송부는 클라이언트 프로세스를 담당한다. (그림 5)는 전용 브라우저의 구성을 나타낸 것이다.

4. 성능 비교 및 분석

실험에 사용된 서버환경은 OS/Server : Windows 2000/

WebServer : IIS, RDBMS : MS-SQL 2000, Application : VB6, ASP, 콘텐츠 파일 전송 : KT컴포넌트1.0를 사용하였다. 또한 클라이언트는 콘텐츠 파일 전송 : KT컴포넌트1.0, 브라우저 : 인터넷익스플로러5.5, 전용 브라우저, Application : VB6, ASP을 사용하였다. 서버콘텐츠 구성은 데이터는 mpeg 형식의 개인 학습 지원용 강의 파일이며, 암호화는 RSA 암호화 알고리즘 및 XOR 연산 기법 사용하였다.

한국소프트웨어진흥원의 2002년 디지털콘텐츠 산업 현황 및 전망 보고서에서 국내의 디지털콘텐츠 산업의 2001년 총 매출액 규모는 약 3조 4,000억 원이며 영상(16.9%), 교육(11.8%), 게임(27.8%) 등 세 분야가 전체 매출액의 55.7%를 차지하고 있다. 특히, 콘텐츠 전송 시스템으로 제공되는 AOD, VOD, eBook 등의 주문형 서비스 콘텐츠들의 비중이 점점 커지고 있다. 따라서 본 연구에서는 제안 시스템에 대해 기존의 시장에서 가장 큰 비중을 차지하고 있는 e-book 서비스 시스템, AOD(Audio On Demand) 시스템, 멀티미디어 동영상 콘텐츠 서비스 시스템과 저작권 보호를 위한 성능을 비교 분석한다.

<표 1> eBook 시스템과 저작권 보호 성능 비교

항목	시스템	권한 옵션 판매 방식	에버북 닷컴	바로북	제안 시스템
인증방식		권리증서 파일	권리증서 파일	동적사용권 + 인증 키	공개키 방식
전송 공격 대비		△	△	○	○
키 노출 대비		△	△	○	○

<표 2> AOD 모델과 비교

항목	시스템	SecuMAX	Digicap	DLC 시스템	제안 시스템
인증방식		개인용 암호키	Token	동적 사용권	공개키 방식
불법유통방지		△	△	△	○
암호화갱신		×	×	×	○
키 노출대비		×	×	×	○

<표 3> 멀티미디어 콘텐츠 제공 시스템과 비교

항목	시스템	FREELEC	eMoney Academy	제안 시스템
암호화된 콘텐츠 제공		×	×	○
안정된 콘텐츠 제공		△	△	○
불법복제/유통 방지		•	•	○
키 노출 대비책		×	×	○
재암호화 여부		•	•	○

<표 1>는 eBook 서비스 시스템과 제안한 시스템의 저작권 보호 성능을 비교한 것이다. eBook 서비스 시스템은 모두 불법 복제와 불법 유통에 대한 대비책을 갖추고 있다. 그러나 인증 방식으로 권리 증서 파일을 이용한 권한 옵션

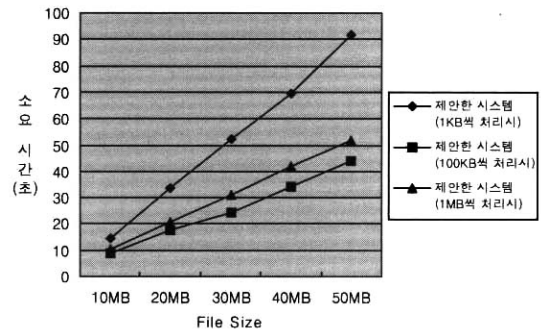
판매 방식과 에버북닷컴 시스템은 전송 시 공격과 키의 유출에 대한 대비책이 확실치 않다. 이에 반해 바로북의 전송 시스템은 인증 방식으로 서버가 클라이언트의 사용권을 확인하는 동적사용권 방식과 인증키 방식을 혼합하여 사용한다. 그러므로 크래커가 키를 입수하거나 전송 중에 콘텐츠를 가로채어도 사용할 수 없다.

<표 2>는 MP3 전송을 위한 AOD 모델들과 제안시스템의 저작권 보호 성능을 비교한 것이다. AOD 모델들은 MP3 파일이나 키를 유포하였을 때 불법 유통 방지 능력을 거의 갖추고 있지 않다. 이에 반해 제안한 시스템은 불법 배포가 불가능한 개인의 비밀키를 이용하기 때문에 불법 유통을 방지할 수 있다. 또한 콘텐츠 재생이 끝나면 암호키를 갱신하므로 불법 유통에 대한 대비책이 확실하다고 할 수 있다. SecuMax 시스템과 Digicap 시스템은 암호화된 MP3 파일을 전송할 때 네트워크 상에 노출되어 있기 때문에 크래커가 MP3를 가로챌 수 있다. 하지만 제안한 시스템은 해당되는 구매자만의 공개키로 암호화하여 전송하기 때문에 크래커가 파일을 가로채더라도 사용할 수 없다. AOD 시스템들이 사용자 인증을 위한 키를 전송할 때 키가 노출되기 때문에 크래커가 이를 가로채 사용할 수 있다. 하지만 제안한 시스템은 이에 대한 대비책으로 사용자 인증에 구매자의 비밀키를 이용하기 때문에 크래커가 가로채기를 하여도 사용할 수 없다.

<표 3>은 멀티미디어 동영상 콘텐츠 제공 시스템과의 저작권 보호 성능을 비교한 것이다. 프리렉과 eMoney Academy는 콘텐츠 다운로드 서비스를 제공하지 않기 때문에 콘텐츠의 불법 복제와 불법 유통을 원천적으로 방지할 수 있다. 그러나 인터넷을 사용할 수 없는 곳에서는 서비스를 받을 수가 없고 인터넷의 전송 속도가 느린 경우에는 안정된 콘텐츠 제공을 보장받기 어렵다. 사용자의 인증은 웹 페이지에 접속하여 로그인하는 것으로 이루어진다. 버록 시스템이 동일시간에 하나의 ID만이 접속할 수 있게 설계되었지만 사용자가 ID와 비밀번호를 타인과 공유함으로써 여러 사람이 서로 다른 시간대에 이용이 가능한 단점을 갖는다. 결국 기존의 대부분의 멀티미디어 제공 시스템의 경우 개인의 아이디와 패스워드만으로 인증이 이루어지기 때문에 디지털콘텐츠의 보호가 거의 이루어지지 않고 있다고 할 수 있다. 하지만 성능 비교 분석 결과와 같이 제안한 시스템이 기존 시스템보다 콘텐츠 불법 복제 및 유통, 콘텐츠 전송 시 공격, 키 노출 등에 대한 대비책을 잘 갖추고 있어 안전하고 효율적인 디지털콘텐츠의 전송이 가능한 것을 알 수 있다.

(그림 6)은 <표 1>의 실험 시스템에서 고용량의 MPEG 파일에 대한 읽고 쓰기 크기에 따른 복호화 수행 시간을 비교한 것이다. 실험결과 파일의 용량에 따라 수행 시간이 6초에서 48초 이상 차이를 보인다. 또한 1KB씩 읽고 쓰기를

처리하는 경우 20MB 이상의 MPEG 파일 용량의 처리는 복호화 수행 시간의 증가로 사용자에게 큰 불편을 초래할 수 있다. 따라서 규모가 적은 MPEG 파일의 경우에는 1KB씩 처리 방식의 사용이 가능하나, 고용량의 MPEG 파일 경우에는 100KB와 1MB씩 처리가 효율적이라 할 수 있다.



(그림 6) 복호화 수행 시간 비교

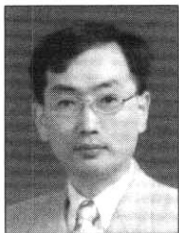
### 5. 결 론

디지털 저작권의 보호는 저작자의 지적인 재산권과 그에 기울인 노력의 보호 측면에서 중요하며 디지털콘텐츠 산업의 발전을 위해 중요하다. 하지만, 디지털콘텐츠는 복제가 용이하고 원본과 복사본이 동일하다는 특성으로 인해 저작권의 보호와 대량 불법 복제 및 불법 유통 방지에 어려움을 겪고 있는 실정이다. 또한 유료화 된 디지털콘텐츠가 인터넷을 통해 전자적으로 거래되는 콘텐츠 전송 시스템이 안정된 수익 모델로서 발전하기 위해서는 적절한 저작권 보호 기술이 요구된다. 본 연구에서는 디지털콘텐츠의 저작권 관리 기술을 기반으로 웹을 통해 안전하고 효율적으로 서비스할 수 있는 디지털콘텐츠 서비스 시스템을 설계하고 구현하였고 제안한 디지털콘텐츠 서비스 시스템의 성능을 기존의 관련 시스템들과 비교 분석하였다. 성능 비교 분석 결과 제안한 시스템이 기존 시스템보다 콘텐츠 불법 복제 및 유통, 콘텐츠 전송 시 공격, 키 노출 등에 대해 효율적인 대비책을 갖추고 있는 것으로 나타났다. 또한 제안한 시스템은 다양한 종류의 콘텐츠에 적용하는 것을 고려하여 설계되었기 때문에 인터넷과 디지털콘텐츠에 관련한 여러 분야에서 효과적인 활용이 가능할 것이다.

### 참 고 문 헌

[1] 한국소프트웨어진흥원, *디지털컨텐츠 중장기 육성전략 수립 사업 연구보고서*, 2000.  
 [2] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transaction on information theory*, Vol. 1T-22, No.6, Nov., 1976.

- [3] Spectral Lines, "Talking About Digital Copyright," IEEE Spectrum, Vol.38 Issue 6, p.9, June, 2001.
- [4] A. O. Freier, P. Karlton and P. C. Kocher, "The SSL Protocol Version 3.0," *www.netscape.com/eng/ssl3*, Nov., 1996.
- [5] ITU-T Rec. X.509, Information technology-Open Systems Interconnection - The Dictionary : Public-key and attribute certificate framework, March, 2000.
- [6] National Bureau of Standard, "Data Encryption Standard," FIPS Pub., 46, 1977.
- [7] Korea Information Security Agency, A Development and Analysis Report on 12bits Block Encryption Algorithm (SEED), 1998.
- [8] R. Rivest, A. Shamir and L. Adelman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, Vol.21, No.2, pp. 120-126, 1978.
- [9] Thorwkrth N. J., Horvatic P., Weis R., Jian zhap, "Security methods for MP3 music delivery," Signals, Systems and Computers, 2000. Conference Record of the Thirty-Fourth Asilomar Conference on, Vol.2, pp.1831-1835. 2000.
- [10] 강우준, 김응모, "디지털 저작권 관리 기술을 이용한 MP3 디지털 음악의 온라인 유통", 정보처리논문지, 제7권 제11호, 2000.



**고 일 석**

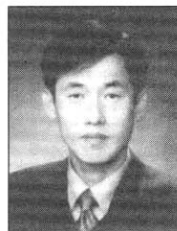
e-mail : isko@ctech.ac.kr  
 경북대학교 컴퓨터공학(공학사/공학석사)  
 미)USIU 경영학과(MBA)  
 연세대학교 컴퓨터산업시스템공학(박사  
 수료)  
 현재 충북과학대학 전자상거래과 조교수

관심분야 : 정보보호, 웹기반시스템의 성능향상, 전략경영



**조 용 환**

e-mail : yhcho@chungbuk.ac.kr  
 고려대학교(이학박사)  
 사) 한국컨텐츠학회 회장  
 현재 충북대학교 전기전자컴퓨터공학부  
 교수  
 관심분야 : .NET Framework, 멀티미디어  
 통신, 트래픽공학, Mobile PKI,  
 정보통신정책



**신 승 수**

e-mail : shinss@chungbuk.ac.kr  
 충북대학교(이학박사)  
 현재 (주)시그마정보기술 연구소장  
 관심분야 : 이미지프로세싱, 의료정보, 영상  
 통신, ATM, 트래픽공학



**조 도 은**

e-mail : harayaa@hanmail.net  
 충북대학교 컴퓨터공학과 박사과정  
 세명대학교 교육대학원 교육학 석사  
 관심분야 : 정보 보안



**권 영 애**

e-mail : aglaia@hanmail.net  
 충북대학교 컴퓨터공학과 박사과정  
 세명대학교 교육대학원 석사  
 관심분야 : 무선인터넷서비스, ATM망,  
 인터넷프로그래밍