암호화 모듈을 적용한 콘텐츠 전송 시스템

박 순 홍*, 최 승 권**, 신 승 수***, 조 용 환****
삼우통신공업(주)*, (주)애니솔루션**, (주)사이젠텍***, 충북대학교****

Contents Transmission System applied by Encryption Module

Park Soon-Hong*, Choi Seung-Kwon**, Shin Seung-Soo***, Cho Yong-Hwan****
Samwoo Telecommunications Co., Ltd.*, ANY Solution Co., Ltd**,
Cyzentech Co.,Ltd. Lab.***, Chungbuk National Univ.****
E-mail : pshong76@hotmail.com, skchoi@anysol.com,
shinss@chungbuk.ac.kr, yhcho@cbucc.chungbuk.ac.kr

요 약

본 논문에서는 암호화 모듈을 적용한 콘텐츠 전송 시스템을 제안한다. 사용자측의 전용 브라우저를 통해 RSA 암호화 알고리즘과 XOR 연산 기법으로 암호화된 콘텐츠를 제공함으로써 콘텐츠 불법 유통과 불법 복제를 방지하고 기존의 콘텐츠 전송 시스템들이 전송 도중의 공격에 취약한 점을 보완한다. 또한 재생 완료 즉시 전용 브라우저로 암호키를 갱신함으로써 콘텐츠와 전용 브라우저를 1:1 관계로 묶어 저작권을 보호한다.

Abstract

In this thesis, we suggest the contents transmission system applied by Encryption Module. It prevents illegal distribution and reproduction of contents and supplements the limitation of the exiting transmission systems during the transmission by providing the contents encoded by RSA encryption algorithm and XOR computation method through user-oriented browser. And at same time, it protects the copyright with typing the contents and user-oriented browser in one-to-one manner by way of using the browser to renew a encoding key as soon as replay is completed.

I. 서론

기존의 콘텐츠 전송시스템들은 개인용 암호키, Token, 동적 사용권, 권리증서 파일 등의 인증 방식으로 불법 복제와 불법 유통 방지를 목적으로 설계되었기 때문에 콘텐츠 전송 도중의 공격에 대한 대응이 미비하였다. 본 논문은 전송할 콘텐츠가 크래커에 의해 조작되는 것을 막기 위해서 콘텐츠의 일부분을 RSA 알고리즘으로 암호화하고 나머지 부분을 XOR 연산 기법으로 암호화는 콘텐츠 전송 시스템을 제안한다. RSA 알고리즘을 콘텐츠 일부분에만 적용함으로써 파일 용량이 증가되는 문제를 해결할 수 있다. 사용자의 콘텐츠 불법 복제 및 유통을 막기 위해서는 콘텐츠를 재생이 끝난 후 다시 암호화하고 개인키를 갱신한다

II. 콘텐츠 암호화

2.1 암호화 알고리즘.

동영상 암호화에는 RSA 알고리즘과 XOR 연산 기법을 사용한다. RSA 기법의 P, Q의 값으로 아주 큰 소수가 요구된다. 이에 따라 평문을 암호화(1byte 단위)한다면 그 데이터는 실험에 사용된 시스템에서 처리할 수 있는 최대치인 double형으로 처리 8byte가 되므로 데이터가 8배 이상으

로 용량이 증가된다. 즉, 10Mbyte의 동영상을 RSA 알고리즘을 이용하여 암호화하면 80Mbyte의 결과물이 생성되는 문제가 발생하게 된다. 이를 해결하기 위해 RSA 알고리즘을 동영상 파일의 처음 100Kbytes까지 적용하였다.

그러나 동영상의 일부분을 암호화하였을 경우 MPEG와 같은 동영상 파일의 특성으로 인해 재생이 가능한 약점이 발생한다. 동영상 파일을 분할할 수 있는 유틸리티를 이용하여 RSA 알고리즘으로 암호화한 100Kbytes 부분을 제거하고 남은 파일의 첫 부분을 헤더 처리하면 재생이 가능하다. 이러한 문제를 해결하기 위해 100Kbytes 이후의 데이터는 XOR를 이용하여 암호화하였다. XOR 연산 기법은 비트 연산의 XOR 연산을 차용하여 원본 데이터의 키 값에 대한 비트들과 데이터의 각 비트들을 XOR 연산을 통해 암호화하고, 암호화된 데이터에 다시 키 값에 XOR 연산을 하여 원본 데이터로 복호화하는 원리를 이용한 것이다. 이를 통해 간단하게 암호화 작업을 수행할 수 있고 성능과 파일 크기에 큰 영향을 끼치지 않게 된다. 또한 XOR 연산 시 여러 개의 키 값을 사용하여 XOR 암호화 과정을 여러 번 수행하면 더욱 견고한 암호화를 거치게 된다.

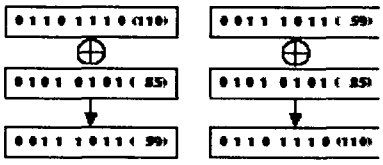

그림 1. XOR 암호화 및 복호화 과정

그림 2는 MPEG 포맷인 동영상 콘텐츠 파일을 RSA 알고리즘과 XOR 연산을 사용하여 PMPEG로 암호화하는 알고리즘을 나타낸다.

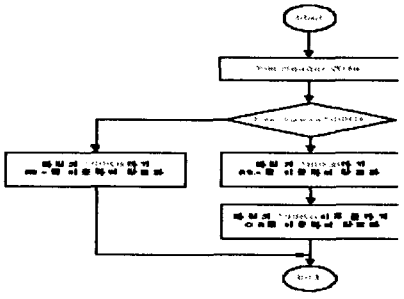

그림 2. MPEG 파일의 암호화 알고리즘

그림 3은 PMPEG로 암호화된 파일을 RSA 알고리즘과 XOR 연산을 사용하여 원래의 MPEG로 복호화하는 알고리즘을 나타낸다.

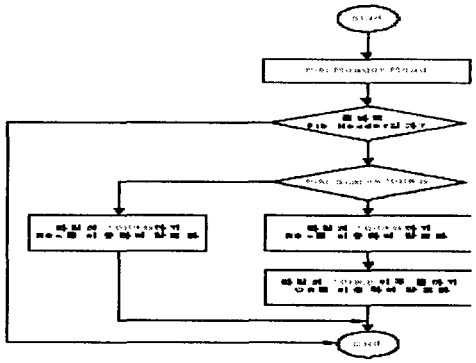

그림 3. PMPEG 파일의 복호화 알고리즘

2.2 콘텐츠 암/복호화 수행 과정

사용자가 콘텐츠를 구매요청 할 경우 RSA 암호화 알고리즘과 XOR 연산을 수행하여 암호화한 콘텐츠를 전송한다. 사용자가 전용 브라우저를 통해 전송 받은 콘텐츠를 재생시키면 전용 브라우저는 콘텐츠를 RSA 복호화 알고리즘과 XOR 연산을 통해 원본 콘텐츠로 변환한 후 재생한다. 재생이 종료되면 불법 복제 방지를 위해 전용 브라우저는 콘텐츠를 다시 콘텐츠를 암호화한다. 콘텐츠의 암호화 및 수행 과정은 다음과 같다.

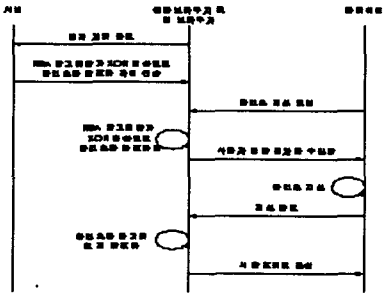

그림 4. 콘텐츠 암호화 수행 과정

1) 사용자로부터 구매를 요청 받음
2) RSA 암호화 알고리즘과 XOR 연산을 사용하여 콘텐츠를 암호화함
3) 사용자가 전송 받은 데이터를 재생하기 위해 플레이어의 재생 버튼을 클릭함
4) 전용 브라우저가 RSA 암호화 알고리즘과 XOR 연산을 사용하여 콘텐츠를 복호화함
5) 전용 브라우저가 사용자 인증 절차를 수행함
5) 플레이어가 콘텐츠를 재생함
6) 재생 종료 후 전용 브라우저가 콘텐츠를 재 암호화함
7) 사용자키를 갱신함

Ⅲ. 지능형 콘텐츠 전송 시스템 설계

3.1 콘텐츠 전송 시스템 구성

본 논문에서 제안하는 콘텐츠 전송 시스템의 핵심 구성 요소는 콘텐츠 전송 서버, 전용 브라우저, 암호화된 콘텐츠와 콘텐츠 제공 업체 측 서버, 지불처리시스템 등으로 구성된다

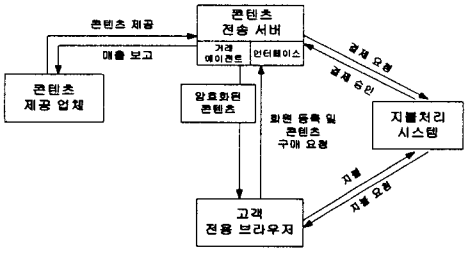

그림 5. 콘텐츠 전송 시스템의 구성 요소

콘텐츠 제공 업체는 콘텐츠 판매자에게 콘텐츠를 제공하고 실시간 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. 새로운 고객이 등록을 하게되면 고객 전용 브라우저를 전송하고 설치하게 한다. 고객의 콘텐츠 구매 요청이 들어오면 지불 처리 시스템에게 결제를 의뢰한다. 결제가 승인되면 해당 콘텐츠를 전송하고 판매 상황을 업체에 통보한다.

지불처리 시스템은 콘텐츠 전송 서버로부터 결제 요청을 받게 되면 해당 고객에게 지불을 요청한다. 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 전송받아 재생한다.

암호화된 콘텐츠는 대칭키를 이용하여 암호화된다. 사용자로부터 구매를 요청 받으면 다시 사용자의 공개키로 암호화하여 전송한다. 사용자가 전송 받은 콘텐츠를 재생하기 위해 전용 브라우저에 내장되어 있는 플레이어의 재생 버튼을 클릭하면 전용 브라우저가 개인키와 대칭키를 이용하여 복호화한다. 재생이 종료되면 전용 브라우저가 즉시 콘텐츠를 공개키로 암호화하여 콘텐츠를 암호화 상태로 관리하게 된다. 사용자는 새로운 개인키를 부여받는다.

3.2 전용 브라우저의 설계

1) 전용 브라우저의 요구 사항

①시스템 서버의 콘텐츠를 열람할 수 있는 기능

②개인 정보 송신과 콘텐츠 수신 기능

③암호화/복호화 기능

④플레이어와 유기적 관계 형성

⑤콘텐츠 재생 시 서버와의 연결을 통해 정식 사용자 확인 기능

⑥동일 네트워크 상의 동시 사용 여부 체크 기능

2) 전용 브라우저의 구성 및 설계

전용 브라우저는 서버 측의 암호화 프로그램과 클라이언트 서버의 관계를 갖는다. 그러므로 전용 브라우저를 설계하기 위해서는 서버 측의 암호화 프로그램을 고려해야 한다.

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.

전용 브라우저는 크게 고객 인터페이스부, 암/복호화부, 전송부로 나누어볼 수 있다. 고객 인터페이스부는 파일 콘트롤창, 콘텐츠 파일 재생, 고객 특화 서비스 수신창 등으로 구성된다. 암/복호화부는 콘텐츠 재생 전에 파일을 복호화하고 재생이 끝나면 암호화를 한다. 전송부는 클라이언트 프로세스를 담당한다

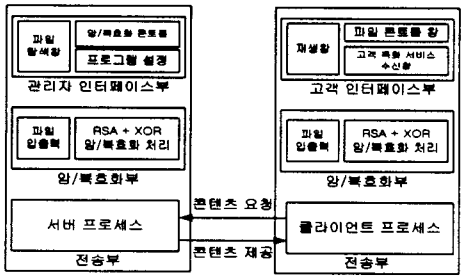

그림 6. 전용 브라우저의 구성

Ⅳ. 실험 및 결과 분석

4.1 암호화 구현

암호화는 서버 측의 콘텐츠 암호화 프로그램과 클라이언트 측의 전용 브라우저로 나누어 구현하였다. 서버 측의 암호화 프로그램은 가상 강의를 제공하는 동영상 파일을 암호화하여 저장을 하고, 이를 클라이언트 측으로 전송할 수 있는 환경을 제공하는 프로그램이다. 클라이언트 측의 전용 브라우저는 암호화된 동영상 파일을 전송 받아서 복호화하

고 재생하는 프로그램이다.

1) 서버측 암호화 프로그램 구현

암호화된 동영상 파일을 전송하기 위한 프로그램 운용 과정은 네 부분으로 구분된다. 첫 번째로 그림 8의 프로그램 폼에서 [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 암호화하여준다. 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.

그림 7. 서버 측 암호화 프로그램 운용 과정

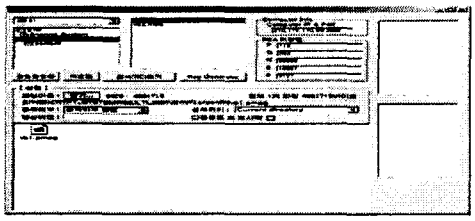

그림 8. 서버 측 PMPEG 전송 프로그램

2) 클라이언트 측 전용브라우저 구현

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 다운로드하게 된다. 재생을 위해 [Play]를 클릭하면 다운로드받은 동영상 파일이 복호화과정을 거쳐 재생된다. 복호화과정은 서버 측 암호화 과정의 역과정을 거친다

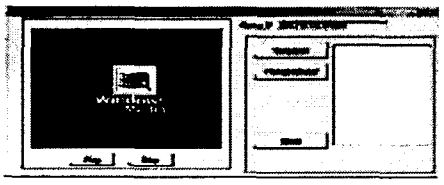

그림 9. PMPEG 전용 브라우저

4.2 비교 분석

1) MP3 저작권 보호를 위한 AOD 모델과의 비교

표 1은 AOD 모델들과 제안한 시스템의 저작권 보호에 대한 성능을 비교한 것이다. AOD 모델들과 제안한 시스템 모두 콘텐츠 불법 복제를 방지할 수 있다. 그러나 AOD 모델들은 MP3 파일이나 Key를 유포하였을 때 불법 유통 방지 능력을 거의 갖추고 있지 않다. 이에 반해 제안한 시스템은 불법 배포가 불가능 한 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 MP3을 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 때에 키가 노출되기 때문에 크래커가 이를 가로채 사용할 수 있다. 제안한 시스템은 이에 대한 대비책으로 사용자 인증에 구매자의 비밀키를 이용하기 때문에 크래커가 가로채기를 하여도 사용할 수 없다.

표 1. AOD 모델과의 저작권 보호 성능 비교

시스템 / 항목	SecuMAX	Digicap	DLC 시스템	제안 시스템
인증방식	개인용 암호키	Token	동적 사용권	공개키 방식
콘텐츠 불법 복제 방지 능력	○	○	○	○
콘텐츠 불법 유통 방지 능력	×	×	△	○
암호화 갱신 여부	×	×	×	○
전송 시 공격에 대한 대비책	×	×	○	○
Key 노출에 대한 대비책	×	×	×	○

(○ : 높음, △ : 낮음, × : 없음, • : 비교 불가)

2) eBook 서비스 시스템과의 비교

표 2는 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. eBook 서비스 시스템과의 저작권 보호 성능 비교

시스템 / 항목	권한 옵션 판매 방식	에버북닷컴	바로북	제안 시스템
인증방식	권리증서 파일	권리증서 파일	동적사용권 + 인증 키	공개키 방식
콘텐츠 불법 복제 방지 능력	○	○	○	○
콘텐츠 불법 유통 방지 능력	○	○	○	○
전송 시 공격에 대한 대비책	△	△	○	○
Key 노출에 대한 대비책	△	△	○	○

3) 멀티미디어 동영상 콘텐츠 전송 시스템과의 비교

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. 비록 시스템이 동일시간에 하나의 ID만이 접속할 수 있게 설계되었지만 사용자가 ID와 비밀번호를 타인과 공유함으로써 여러 사람이 서로 다른 시간대에 이용이 가능한 단점을 갖는다.

표 3 멀티미디어 동영상 콘텐츠 제공 시스템과의 저작권 보호 성능 비교

시스템 / 항목	FREELEC	eMoney Academy	제안 시스템
콘텐츠 제공 여부	×	×	○
안정된 콘텐츠 제공	△	△	○
콘텐츠 불법 복제 방지 능력	•	•	○
콘텐츠 불법 유통 방지 능력	•	•	○
전송 시 공격에 대한 대비책	•	•	○
Key 노출에 대한 대비책	×	×	○
재 암호화 여부	•	•	○

4) 복호화 수행 시간 비교

본 절에서는 기존의 MP3 저작권 보호를 위한 AOD 모델인 SecuMAX, Digicap과 본 논문에서 구현한 전용 브라우저에서 콘텐츠 파일 복호화에 걸리는 시간을 비교하였다. 전용 브라우저의 파일 입출력 처리 크기를 1KB, 100KB, 1MB의 세 가지로 구현하여 비교하였다. 전용 브라우저는 MP3 파일을 비롯한 대부분의 동영상을 처리할 수 있으나 AOD 모델은 MP3 전용 시스템이고 MP3 파일은 대부분 5MB 내외의 용량을 갖기 때문에 용량이 큰 MPEG 포맷의 동영상 파일에 대한 비교는 적합하지 않다. 따라서 구현한 전용브라우저 끼리의 복호화 수행 시간을 비교하였다

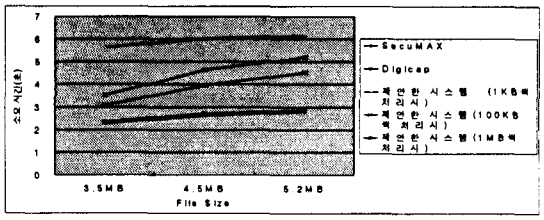

그림 10. AOD 시스템과 제안한 시스템과의 복호화 수행시간 비교

그림 10과 같이 기존의 AOD 시스템들이 제안한 시스템에 비해 복호화 수행 속도가 빠른 것을 알 수 있는데 이는 속도가 빠른 대칭키 방식을 사용하기 때문이다. 1KB씩 읽고 쓰기를 처리할 때보다 100KB씩 처리할 때 성능이 향상되었으나 1MB씩 처리할 때는 오히려 성능이 저하되었다. 100KB씩 읽고 쓰기를 처리하는 전용 브라우저는 AOD 시스템과 비교할 때 사용하는데 큰 불편을 주지 않을 정도인 1.5초 이내의 성능 차이를 보인다. 그러나 1KB와 1MB씩 읽고 쓰기를 처리하는 전용 브라우저는 3~6초 이상 복호화 처리 시간이 소요된다.

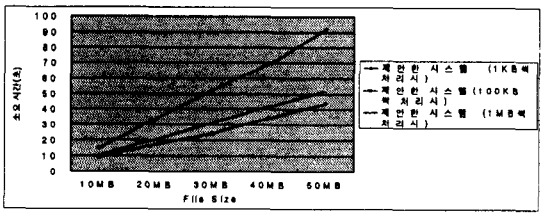

그림 11. 읽고 쓰기 크기에 따른 복호화 수행 시간 비교

그림 11은 제안한 시스템의 전용 브라우저에서 읽고 쓰기 크기에 따른 복호화 수행 시간을 비교한 것이다. MPEG 파일의 용량에 따라 수행 시간이 대략 6초에서 48초 이상 차이를 보인다. 1KB씩 읽고 쓰기를 처리하는 전용 브라우저의 경우 20~30MB 이상의 MPEG 파일 용량의 처리는 고객에게 큰 불편을 초래할 수 있다. 100KB와 1MB씩 처리하는 경우에도 20MB 이상의 파일 용량 처리에는 10초 이상 시간이 소요되지만 최근 많이 이용되는 AVI나 ASF 파일의 경우 상대적으로 용량이 수 배 이상 작으므로 응용이 가능하다.

성능 향상을 위해 100KB와 1MB 사이에서 최고의 성능

을 나타내는 읽고 쓰기의 용량을 찾을 필요가 있다.

V. 결론

본 논문에서는 암호화 모듈을 적용한 콘텐츠 전송 시스템을 제안하였다. 기존의 콘텐츠 전송시스템들은 개인용 암호키, Token, 동적 사용권, 권리증서 파일 등의 인증 방식으로 불법 복제와 불법 유통 방지를 목적으로 설계되었기 때문에 콘텐츠 전송 도중의 공격에 대한 대응이 미비하였다. 제안한 시스템은 전송할 콘텐츠가 크래커에 의해 조작되는 것을 막기 위해서 콘텐츠의 앞 부분을 RSA 알고리즘으로 암호화하고 나머지 부분을 XOR 연산 기법으로 암호화한다. RSA 알고리즘을 콘텐츠 일부분에만 적용함으로써 파일 용량이 증가되는 문제를 해결할 수 있다. 사용자의 콘텐츠 불법 복제 및 유통을 막기 위해서는 콘텐츠를 재생이 끝난 후 다시 암호화하고 개인키를 갱신한다.

제안한 콘텐츠 전송 시스템의 성능을 분석하기 위하여 기존의 시스템들과 비교 분석하였다. 성능 비교 분석 결과 제안한 시스템이 기존 시스템보다 콘텐츠 불법 복제 및 유통, 콘텐츠 전송 시 공격, Key 노출 등에 대한 대비책을 잘 갖추고 있는 것으로 나타났다. 시스템들의 콘텐츠 복호화 소요 시간을 측정해본 결과 대칭키를 사용한 기존 시스템의 속도가 2초 가량 빠른 것으로 나타났으나 사용자가 불편을 느낄 정도는 아니다. RSA 알고리즘과 XOR 연산 기법을 통해 콘텐츠 전송 도중의 공격으로 인한 데이터 왜곡을 방지 할 수 있다는 점이 복호화 속도보다 더 큰 이점이라고 판단한다.

제안한 시스템은 다양한 종류의 콘텐츠에 적용하는 것을 고려하여 설계되었기 때문에 인터넷과 디지털 콘텐츠에 관련한 여러 분야에서 활용이 가능할 것이다

참 고 문 헌

[1] Thorwkrth, N.J., Horvatic, P., Weis, R., Jian zhap, Security methods for MP3 music delivery", Signals, Systems and Computers, 2000

[2] 강상승 외, MP3 미디어 데이터의 온라인 유통기술 , 한국전자거래학회/한국정보시스템 학회 종합학술대회논문집, pp.589-600, 1999.

[3] 강우준, 김응모, 디지털 저작권 관리 기술을 이용한 MP3 디지털 음악의 온라인 유통 , 정보처리학회논문지, 제7권 제11호, 2000.

[4] 윤우성, 김태윤, UML을 이용한 불법 복제 방지를 위한 ESD 서버 설계 , 정보처리학회 춘계학술발표논문집, 제7권 제1호, 2000.

[5] 이용효, 황대준, 에이전트 기반의 동적 디지털저작권 관리시스템 설계 및 구현 , 정보처리학회논문지, 제8-D권 제5호, 2001.