디지털산업정보학회 논문지 제5권 제2호-2009년 6월

시스템 인증기법을 적용한 DRM 시스템 설계 및 구현

장 은 겸* · 이 범 석**

A Design and Implementation of DRM System by Applying System Authentication Method

Jang, Eun Gyeom · Lee, Bum Suk

〈Abstract〉

The digital contents distribution system via network provides comfortability, usability, and diversified functions to content's users. However, for the characteristic of easy access of digital contents, the copyright infringements and indiscreet contents distribution are realized in this days. In other words, any users with the authentication key can access to copyright contents with any restrictions. To solve this problems, we proposed a user authentication mechanism which prevent indiscreet access to the digital content by using user system information. Also, to provide safe distribution of digital content, we used user's unique content authentication key.

Key Words : Access Control, DRM, Authentication, Copyright Protection

Ⅰ. 서론

정보통신기술의 발달로 인하여 공공 및 민간분야에 정보시스템 사용이 증가하고 있는 반면 인터넷 등 개방형 정보통신망과의 상호접속으로 인한 정보의 유출, 파괴, 위·변조, 바이러스 유포 등 각종 해킹 및 컴퓨터 범죄가 증가하고 있다.

인터넷과 같은 개방형 시스템 환경에서 호스트들이 네트워크를 통하여 상호 연결되어 있으며 다양한 사용자가 자원을 공동으로 활용되고 있다. 이러한 개방형 시스템의 오픈된 특성과 디지털콘텐츠 복제의 용이성은 누구나 사용할 수 있는 편이성과 가용성을 제공한다. 이러한 특성을 이용하여 디지털콘텐츠의 무분별한 사용 및 불법 복제, 무단도용의 문제가 발생한다.

P2P 방식을 지원하는 소리바다 및 겜플 서비스 등은 실제 저작물을 사용자가 보유하고 있고, 로그인 되어 있는 사용자와 사용자간에 정보를 주고받을 수 있는 중계업자 역할을 하고 있다. 최근 이러한 P2P 서비스를 통해 '워낭소리'와 같은 영화가 불법적으로 유통되어 제작자는 엄청난 피해를 입은 사례를 갖고 있다. P2P 서버에 대한 불법 저작물 유통 시스템에 대한 서비스는 지금도 법적인 공방이 이루어지고 이러한 문제를 해결하기 위해 범국민적인 홍보 및 법적보호를 취하고 있고 불법적인 저해 요인을 파악하여 대응방법을 강구하고 있다. 디지

* 대전대학교 컴퓨터공학과 겸임교수
** 혜천대학 유아교육과 부교수

털콘텐츠의 저작권을 보호하기 위한 기술로는 워터마킹 기술을 사용하고 있고, 저작물의 유통 및 배포, 사용 권한에 따른 보호기술로 DRM(Digital right management)이 있다.

현재 개발된 DRM 기술은 크게 두 가지로 분류된다. 하나는 디지털콘텐츠 전체 유통 프로세스와 암호화, 네트워크, 정보관리 등 핵심 정보기술을 결합한 "시스템 기반형" 이며 다른 하나는 암호화, 워터마킹 등 요소기술을 활용한 "요소기술 기반형"이 있다. DRM은 21세기 신산업으로 각광을 받고 있는 디지털콘텐츠 산업의 기반을 구축하는데 필수적인 디지털콘텐츠의 저작권보호 및 유통 인프라 시스템을 구축하는데 필수적인 기술로써 워터마킹, 문서보호 솔루션등과 함께 디지털콘텐츠를 불법복제 및 사용으로부터 보호할 수 있는 솔루션 가운데 하나이다[1, 2].

워터마킹 기술은 자체가 불법복제 및 유통된 콘텐츠에 저작권을 보호하기 위한 기술을 제공하는 반면, DRM은 콘텐츠의 불법 사용자체를 원천적으로 방지할 수 있는 것이 특징이다. 암호화 기술을 이용해 디지털콘텐츠를 패키지 형태의 암호화된 데이터로 변환시키는 DRM 솔루션은 디지털콘텐츠가 유통된 후 사용자권한 영역에 제한되어 솔루션이 제공된다. 그러나 콘텐츠에 정상적인 인증키를 획득한 사용자는 무한으로 복제품을 만들어 유포할 수 있다[3, 4].

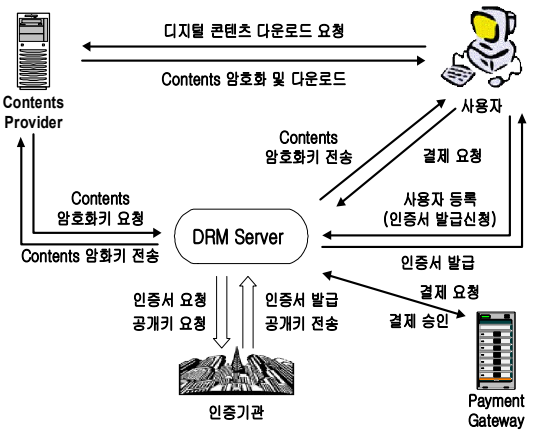
이러한 문제로부터 디지털콘텐츠를 보호하기 위해 본 논문에서는 사용자 영역의 시스템 인증정보를 이용하여 디지털콘텐츠의 접근을 통제하고 관리하여 안전한 디지털콘텐츠 유통망을 지원하도록 하였다.

II. 디지털콘텐츠 보호 및 관리 기술

2.1 디지털콘텐츠 관리 기술 분석

인터넷을 통한 디지털콘텐츠산업은 다양한 콘텐츠를 손쉽고 편리하게 접근하고 CP/ISP는 디지털콘텐츠 공급과 동시에 콘텐츠 저작권 관리와 보호를 위한 기술을 요구한다.

DRM 기반의 디지털콘텐츠 관리기술은 사용자를 인증하고, 인증된 사용자만이 CP/ISP와 협약된 콘텐츠 제어범위 내에서 이용을 허용하는 기술이다. <그림 1>은 공개키 기반의 디지털콘텐츠 관리 유통구조를 보인다.



<그림 1> 공개키 기반의 콘텐츠 관리 유통구조

디지털콘텐츠는 CP/ISP에 의해 사용자에게 제공된다. 콘텐츠를 필요로 하는 사용자는 인증기관에 의해 신분을 확인하는 인증서를 요청하여 발급 받는다. 인증서를 발급 받은 사용자만이 디지털콘텐츠를 이용할 수 있는 자격을 갖추고, CP/ISP에서 제공하는 콘텐츠를 사용할 수 있다. 다운로드 및 사용권한을 획득하기 위해서는 개인인증서를 통해 신분 확인 후 결제처리가 이루어진다. 또한, 사용권한을 획득한 사용자는 암호화된 디지털콘텐츠를 해독할 수 있는 키를 획득하여 사용이 가능하다. 즉 인터넷에서 제공되는 디지털콘텐츠는 사용자 인증을 위해 인증기관에 의해 신분 확인 후 DRM 서버에 의해 콘텐츠가 보호되어 사용자에게 제공되는 유통구조를 가진다[5-7].

그러나 디지털콘텐츠 보호를 위한 기술로 관용암호화 방식을 이용하여 키 교환을 통해 콘텐츠가 제공된다. 콘

<표 1> 콘텐츠 보호 기술요소

항 목	설 명
Contents Encryption	• 암호화 알고리즘을 이용하여 콘텐츠를 암호화하여 사용자에게 안전하게 전달하고 재생시 복호되어 제공 • 복호키는 인증된 사용자에게만 제공
Usage Rule	• 사용자의 요구 및 권한에 의한 콘텐츠 사용제한, Contents Provider의 다양한 마케팅 전략에 의해서 다양한 콘텐츠 Rule을 적용
Persistent Protection	• 콘텐츠 이용은 전 유통과정을 통해 business rule의 조건에 따라 지속적으로 제어 • 콘텐츠 사용권한으로 콘텐츠 자체를 변경 및 복제, 사용권한 제어정보변경으로부터 보호.
Trusted Environment	• 저작권을 피해가기 위해 DRM의 모듈 일부를 변경 및 대체로부터 보호 • 정상적인 제품임을 보증하는 인증 절차와 모듈이 손상되거나 대체되지 않았음을 증명하는 기술
Super distribution	• 콘텐츠 사용자가 자신이 구입한 콘텐츠를 E-mail, CD-ROM, 디스켓 등을 통해 다른 사람에게 반복적으로 배포할 수 있게 하여 콘텐츠의 급속한 확산을 가능하게 하는 유통기술
Value-chain Support	• 디지털콘텐츠의 최초 생산한 소유자(Content Owner), 배급자(Content Distributor), 판매자(Content Provider)가 콘텐츠의 전자상거래를 위해 복잡한 유통 구조를 시스템화하기 위한 다양한 value-chain 방식이 적용

텐츠는 한 번의 신분확인을 통해 모든 권한을 주는 결과를 초래하고 불법복제 및 허가되지 않은 사용자의 접근, 불법수정 등의 문제를 일으킬 수 있다. 그러므로 본 제안 시스템은 콘텐츠 자체보호를 위한 방법으로 전용 재생기를 이용하여 디지털콘텐츠를 안전하게 보호하고 사용자별 사용권한 영역에 따라 다양한 서비스를 지원한다.

2.2 디지털콘텐츠 보호 기술요소

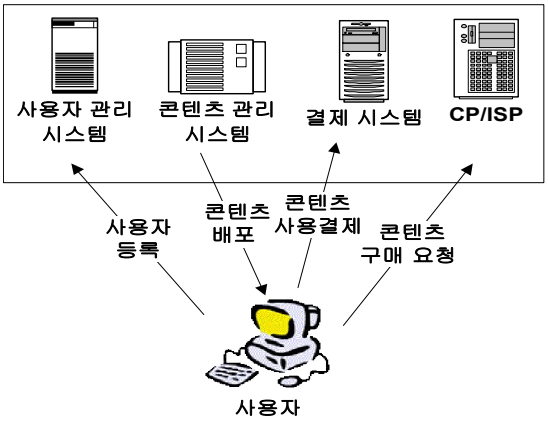
DRM은 다양한 채널을 통해 유통되는 전자서적, 음악파일, 영상 정보, 게임, 소프트웨어, 이미지 등의 각종 디지털콘텐츠 서비스의 유료화를 가능하게 하는 기술이다.

디지털콘텐츠가 생성될 때부터 배포되어 이용될 때까지의 전체 라이프 사이클에 걸쳐 적용되며, 각각의 사용자가 사전에 정해진 조건을 만족해야만 이용할 수 있는 장치로써, 콘텐츠의 자유로운 유통은 허용하지만 불법사용은 철저히 막는 기술이다. DRM은 단순히 불법복제만을 막는 기술이 아니라 안전한 저작권과 승인 내역, 권리와 승인의 집행, 인증된 환경과 서비스 인프라 등을 가능하게 하는 하드웨어와 소프트웨어를 모두 포함한 디지털 저작권 관리에 관한 기술, 절차, 처리, 알고리즘 등을 의미한다[5, 6]. <표 1>은 콘텐츠 보호를 위해 필요한 기술요소이다.

Ⅲ. 디지털콘텐츠보호 접근통제 시스템

3.1 시스템 구성

<그림 2>는 제안 시스템의 디지털콘텐츠 유통 구성도로서 사용자와 CP/ISP간에 콘텐츠를 배포하고 유통/관리하는데 필요한 인터페이스 관계를 나타낸다.



<그림 2> 시스템 구성도

사용자는 콘텐츠 사용을 위해 시스템에 사용자등록을 수행하고 콘텐츠 활용에 따른 결제금액을 지불 한다. 결제된 콘텐츠는 사용자에게 배포된다.

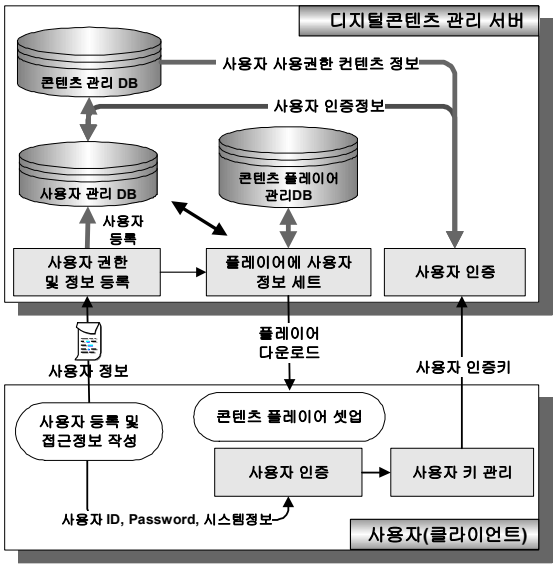
사용자등록은 사용자의 ID와 패스워드를 포함한 기본 신상정보를 요구한다. 본 제안시스템에서는 사용자의 고

유 ID와 패스워드를 통해 사용자를 인증하고, 2차로 사용자가 디지털콘텐츠를 사용할 시스템정보를 등록한다. 시스템정보는 CD-ROM, 하드웨어, CPU의 고유 식별번호이다.

3.2 사용자인증 관리

콘텐츠관리 서버와 사용자시스템은 실시간 사용자인증 인터페이스가 제공된다. On/Off -Line 상에서 사용자 권한정책을 체크하여 사용자를 인증한다. <그림 3>은 사용자 인증관리 과정을 보인다.

사용자 인증관리 모듈에서 인증정보를 생성하여 발급받는 경우는 두 가지 경우로 나눈다. 첫 번째는 처음 사용자 등록시 인증 정보 발급 부분과 두 번째는 유효기간 및 사용자 콘텐츠 구매에 의한 정책 변경시 인증을 한다. 후자는 발급 받은 인증 정보 재발급시에 발생하는 경우로써 기존 인증정보에 변경 내용이 발생하였을 경우에 행해진다. 또한 인증정보의 유효기간이 초과 하였을 경우, 인증정보 자체 파기에 의해 인증정보가 변경된다.



<그림 3> 사용자 인증관리 과정

사용자의 고유 ID와 패스워드는 서버의 사용자관리 데이터베이스에 등록되어 관리된다. 또한 사용자는 콘텐츠 플레이어를 다운받아 설치하고 플레이어를 이용하여 사용자인증정보가 세팅된다. 즉 사용자 ID와 패스워드는 사용자인증을 위한키로 사용되며 또한 사용자 영역의 시스템정보에 의해 인증이 이루어진다. 이 시스템정보는 사용자시스템의 CPU, 하드디스크, CD-ROM의 고유 식별정보로서 결제가 이루어진 콘텐츠의 접근키로 활용된다.

범용적인 DRM을 적용하기 위해 디지털콘텐츠의 환경정보를 포함하는 헤더필드를 암호화하여 접근통제 기능을 제공한다. 즉, 헤더필드만을 암호화하여 사용자에게 제공하고 사용자 식별코드와 시스템정보를 이용한 암호화키를 이용하여 콘텐츠에 접근을 허용한다. 암·복호화키는 다음과 같이 생성된다.

$$E_k = ID_{user} \oplus CPU_{ID} \oplus HDD_{code} \oplus CDROM_{ID}$$
$$If\,(Size(E_k) > 128bit)\ Then\ Front\ 128bit\ used;$$
$$Else\quad E_k + Pading(0);$$

콘텐츠 헤더필드 암호화키는 사용자 ID를 포함한 시스템정보를 이용한다. 사용자 ID(ID_{user})와 시스템정보(CPU_{ID}, HDD_{CODE}, $CDROM_{ID}$)가 128bit 미만인 경우에는 '0'값으로 Padding 되고 초과된 경우에는 코드 앞부분의 128bit만을 활용한다. 연산결과로 생성된 인증키는 암호·복호화 적용되는 키로서 128bit 크기를 갖는다. 암호 알고리즘은 128 비트의 대칭형 키 블록 SEED를 적용한다.

3.3 디지털콘텐츠 암·복호화 과정

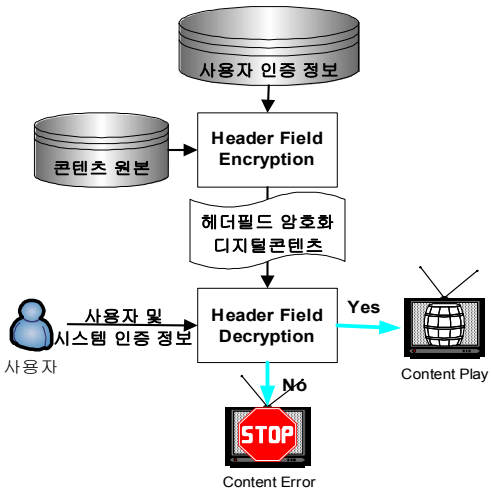
콘텐츠관리 서버와 사용자영역의 콘텐츠 관리 에이전트는 사용자 인증과 콘텐츠 보호에 서로 연계 관계를 갖는다.

디지털콘텐츠관리 서버로부터 전송된 콘텐츠는 디지

털콘텐츠관리 에이전트에 의해 관리된다. 즉, 콘텐츠 헤더필드가 암호화된 콘텐츠는 사용자 권한영역 내에서 복호키를 이용한 플레이가 가능하다.

인증은 On/Off-Line 상에서 에이전트에 의해 인증이 이루어진다. <그림 4>는 암호화된 디지털콘텐츠가 사용자에게 공급되는 과정을 보인다.

사용자영역의 에이전트는 사용자 ID와 시스템정보를 이용하여 키를 생성하고, 생성된 키를 이용하여 암호화된 헤더 필드를 복호한다. 헤더 필드가 복호된다는 것은 디지털콘텐츠의 접근권한이 허용되었다는 것을 의미한다.



<그림 4> 디지털콘텐츠 암·복호화 과정

Ⅳ. 제안 시스템 실험 및 성능 평가

4.1 성능 실험 주요항목 및 시나리오

성능실험은 다음 항목을 중심으로 테스트한다.

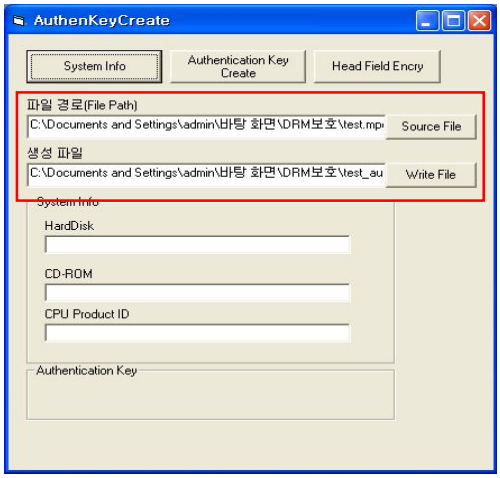
- 인증 받지 못한 사용자에 대한 콘텐츠 보호
- 불법복제에 의한 콘텐츠 보호
- 사용자 및 시스템 인증에 의한 안전한 콘텐츠 제공

위에 제시한 항목을 중심으로 디지털콘텐츠의 안전성을 보장하기 위해 사용자 및 시스템 인증을 위한 인증키 생성과 생성된 인증키에 의한 디지털콘텐츠 헤더 암호화, 인증여부에 의한 디지털콘텐츠 플레이 사항을 시나리오로 작성하여 실험한다. 또한 불법복제가 이루어져 유포되었을 때, 범용 디지털콘텐츠 플레이어에서의 안정성을 제공하는가를 실험한다.

4.2 디지털콘텐츠 인증키 적용

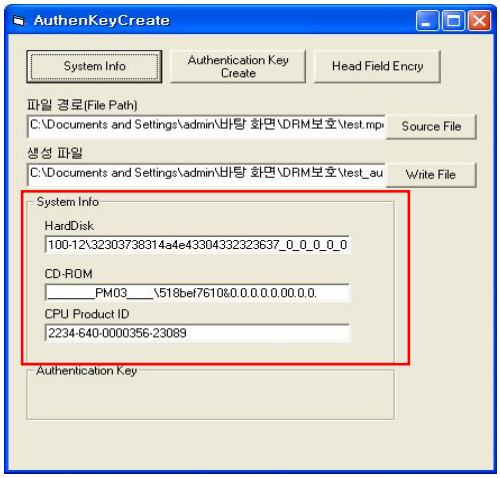
인증키는 사용자 시스템의 정보를 활용한다. 3.2절에서 기술한 수식을 이용하여 인증키를 생성한다.

<그림 5>는 사용자 인증키 생성을 위한 기본 프로그램 설정화면이다. 파일 경로는 원본 콘텐츠이고 생성 파일은 인증키를 적용하여 생성된 콘텐츠이다.



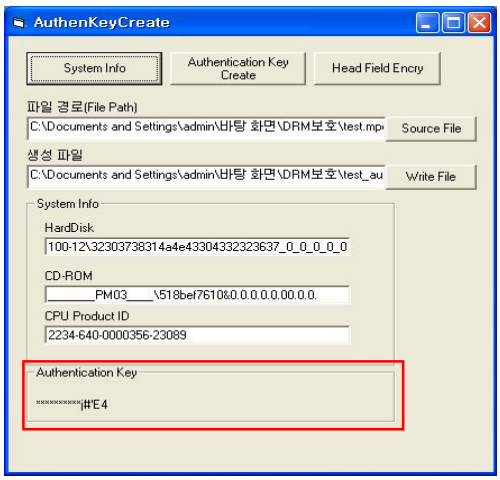
<그림 5> 인증키 생성 기본 환경

"System Info"는 시스템정보 추출기능을 제공한다. 이 기능에 의해 <그림 6>와 같이 사용자시스템의 정보인 "Hard Disk", "CD-ROM", "CPU Product ID" 값을 추출한다.



<그림 6> 사용자 시스템정보 추출

추출된 시스템정보는 "Authentic- ation Key Create"에 의해 인증키 값이 생성되는데 시스템정보와 사용자 ID 값을 포함한다. 인증키 값은 <그림 7>과 같이 128bit(16byte)로 생성된다.



<그림 7> 인증키 생성

인증키 값은 "Head Field Encry"에 의해 디지털콘텐츠 헤더 영역을 암호화 하는데 키 값으로 적용된다. 이렇게 생성된 콘텐츠는 사용자에게 전송되어 사용자 영역의 에이전트에 의해 사용자를 인증하고 플레이된다.

4.3 디지털콘텐츠 플레이

사용자 인증키로 암호화된 디지털콘텐츠 헤더 영역은 실시간으로 복호되어 디스플레이가 이루어진다. 사용자가 등록한 시스템정보와 사용자 ID가 인증이 되어야 접근권한이 부여된다.

에이전트는 DRM 서버로부터 제공받은 콘텐츠의 헤더를 복호화하기 위해 인증키를 생성한다. 인증키는 사용자가 시스템 로그인시에 입력한 ID와 디지털콘텐츠가 플레이되는 시스템의 정보의 키 조합에 의해 생성된다. 인증이 완료되면 원활한 서비스를 제공 받을 수 있으나 인증 시스템의 정보와 사용자 ID가 인증키와 일치하지 못하면 경고 메시지와 함께 콘텐츠를 활용할 수 없다. <그림 8>은 인증이 이루어진 콘텐츠의 플레이 화면이고 <그림 9>은 인증키가 불일치할 때 발생하는 화면이다.

<그림 8> 인증된 콘텐츠 플레이

<그림 9> 인증키 불일치 콘텐츠 플레이

인증키 불일치 경우는 등록한 시스템 인증 정보 또는 사용자 ID가 일치하지 않을 때 발생하며 만약 사용자가 등록한 시스템이 아닌 다른 시스템에서 결제한 콘텐츠(접근 권한이 허용된 디지털콘텐츠)를 보고자할 때에는 시스템정보를 다시 등록하여 인증키를 생성하여 디지털 콘텐츠에 적용한다.

제안 시스템 모델은 콘텐츠 플레이를 위한 에이전트를 필요로 한다. 전용 재생기인 에이전트 영역에서는 콘텐츠의 불법적인 접근으로부터 보호되나 일반 범용 디지털콘텐츠 플레이에서 콘텐츠가 보호되는지를 실험하였다. 실험 화면은 <그림 10>과 같다.

<그림 10> 범용 디지털콘텐츠 플레이어

범용 디지털콘텐츠 플레이어는 곰 플레이어를 활용하였다. 범용 플레이어에서는 플레이하고자하는 콘텐츠의 헤더의 정보를 얻을 수가 없어서 플레이가 불가능한 에러 메시지를 보였다. 곰 플레이어뿐만 아니라 위도우 미디어 플레이어에서도 같은 결과를 얻었다.

4.4 성능평가 분석

제안 시스템은 사용자의 시스템정보와 사용자 ID를 기반으로 128bit 키를 생성하여 디지털콘텐츠의 헤더를 SEED 암호화 알고리즘으로 암호화하였다. 디지털콘텐츠에서 헤더정보는 콘텐츠의 포맷을 결정짓는 중요한 요소이다. 또한 헤더정보에 의해 콘텐츠의 종류, 콘텐츠 플레이시에 적용되는 환경 및 요소 등의 정보에 의해 콘텐츠의 원활한 플레이가 가능하다. 즉, 디지털콘텐츠의 헤더를 보호하는 것은 콘텐츠의 접근에 간단하면서도 효율적인 보호기법이다. 성능실험 시나리오에 의한 제안 시스템 실행 결과는 다음과 같다.

- 범용 디지털콘텐츠 플레이어에서 안전성
  - 콘텐츠 헤더 암호화에 의해 콘텐츠 보호
  - <그림 10>의 실험 결과
- 사용자 영역의 시스템 인증
  - 시스템정보와 사용자 ID에 의해 인증키가 제공되어 콘텐츠 접근
  - <그림 8>의 실험 결과
- 암호화된 콘텐츠 헤더의 안전성
  - SEED 블록 암호화 알고리즘의 안전성에 준한다.
- 무분별한 콘텐츠의 불법복제 방지
  - 불법적으로 콘텐츠가 복제되어도 시스템정보를 포함하는 인증키가 없어 접근이 통제
  - <그림 9>의 실험 결과

V. 결론

이러닝의 학습 콘텐츠, 영화, UCC 등을 포함한 다양한 디지털콘텐츠의 보급으로 인해 쉽고 빠르게 지식 및 정보를 얻을 수 있다. 그러나 무분별한 디지털콘텐츠의 복제와 접근으로 재산권에 침해가 발생하고 있다. 이러한 문제를 해결하고자 본 논문에서는 사용자인증을 위해 시스템 인증 기법을 제안하였다.

사용자인증은 사용자정보와 사용자영역의 시스템정보에 의해 생성된 인증키를 이용한다. 인증키로 디지털콘텐츠의 헤더영역이 암호화되어 사용자에게 보급된다. 이렇게 보급된 콘텐츠는 인증키에 의해 복호되어 플레이된다. 반면, 사용자정보 및 시스템정보가 일치하지 않아,

인증 받지 못하여 콘텐츠에 접근할 수 없다. 이러한 특성으로 불법복제콘텐츠의 경우 제안 시스템의 에이전트를 포함한 범용 디지털콘텐츠 플레이어에서도 플레이가 되지 못하여 비인가 영역에 대한 접근으로부터 콘텐츠를 보호하였다.

제안 기술의 사용자인증은 오프라인 환경인 경우 인증정보가 변경되었을 때에는 원활한 서비스가 제공되지 못한다. 그러므로 제안 기술의 사용자인증기술을 온라인 환경의 스트리밍 서비스 영역에 적용한다면 디지털콘텐츠를 안전하게 보호 할 수 있을 것이다.

참고문헌

[1] 박남재 · 송유진, "디지털 컨텐츠 저작권 보호기술", 한국정보보호학회, 2001. 10.

[2] Ant Alltan, "Digital Rights Management Softwore Perspective", Gartner, 2001. 11.

[3] 정사라 · 석종원 · 홍진우, "디지털 컨텐츠의 저작권 관리를 위한 워터마킹 기술", 전자통신동향분석, 제16권 제14호, 2001. 8.

[4] 김현태 · 임재혁 · 김대진 · 원치선, "저작권 보호와 인증을 위한 객체기반 디지털 워터마크", SK Telecommunication Review 제10권 5호, 2000, pp. 1003-1016.

[5] 최혁 · 김태정, "비대칭 워터마킹 시스템에 관한 연구", 한국정보보호학회, 제12권, 제1호, 2002, 2.

[6] 이형우, "안전한 컨텐츠 유통을 위한 방안 연구", 한국정보보호학회, 제12권 제1호, 2002, 2.

[7] 장재혁 · 조배수 · 최용락, "디지털 컨텐츠 보호를 위한 중안 관리 시스템", 한국인터넷정보학회, 제3권 2호 2002.

■ 저자소개 ■

장 은 겸
Jang, Eun Gyeom

2009년 3월~현재
대전대학교 컴퓨터공학과 겸임교수
2008년 3월 M2M Korea 연구소장
2007년 8월 대전대학교 컴퓨터공학과 (공학박사)
2002년 8월 대전대학교 컴퓨터공학과 (공학석사)
2000년 8월 대전대학교 컴퓨터공학과 (공학사)

관심분야 : 정보보호, DRM, 컴퓨터포렌식스
E-mail : jangegu. nate. com

이 범 석
Lee Bum Suk

2008년3월~현재
혜천대학 유아교육과 부교수
1992년3월~2008년 3월
혜천대학 컴퓨터멀티미디어과 부교수
성균관대학교 통계학과 전산통계전공 (박사)
한국외국어대학교 정보처리학과 (석사)

관심분야 : 멀티미디어, 교육공학
E-mail : bslee@hcc. ac. kr

논문접수일 : 2009년 5월 9일
수 정 일 : 2009년 5월 30일
게재확정일 : 2009년 6월 3일