韓國 컴퓨터情報學會 論文誌
第8卷 第3號, 2003. 9.

2003-8-3-1-1

디지털 콘텐츠 유통 및 보호를 위한 인증 시스템 설계 및 구현

고 병 수*, 장 재 혁**, 최 용 락***

Design and Implement of a Certification System for Digital Contents Circulation and Secure

Byoung-Soo Koh*, Jae-Hyuk Jang**, Yong-Rak Choi***

요 약

인터넷의 발달은 디지털 콘텐츠 시장의 활성화를 일으키는 가장 중요한 요소이다. 그러나 콘텐츠의 불법복제와 무분별한 사용은 콘텐츠 시장을 위축시키는 장애요인으로 작용한다. 이러한 콘텐츠의 불법 유통과 불법복제를 사전에 예방할 수 있는 새로운 기술이 필요하다. 본 논문에서는 디지털 콘텐츠 시장의 활성화를 위해 안전한 유통과 저작권 보호를 지원하는 인증 시스템을 제안하였다. 네트워크를 통한 사용자 인증과 사용 횟수에 따라 콘텐츠가 소실되는 모델을 제안하고, 콘텐츠 자체를 필터링하여 제공함으로써 불법 도용의 위험성을 제거하였으며 인터넷을 통한 콘텐츠 유통을 안전하게 보호하는 시스템을 개발하였다.

Abstract

The growth of Internet is the main factor that activates the Digital Contents Market. However the Digital Contents Market could be shrunk by an illegal reprinting and imprudent using. Therefore we urgently need a new technology which can prevent the contents from illegal using, illegal reprinting and imprudent using. We developed the system prohibits a imprudent using in order to activate the Digital Contents Market. We developed the system protects the contents safely by removing the dangerous for the illegal reprinting with providing the encoded contents and the system removes the contents according to the number of usage and the user authentication through Network.

▸ Keyword : 디지털 콘텐츠 보호/DRM/공개키 알고리즘/Watermarking

*, ** 대전대학교 컴퓨터공학과 대학원 ** 대전대학교 컴퓨터공학부 교수
※ 본 연구는 한국과학재단 지역협력연구센터(A-1-3) 지원으로 수행되었음.

Ⅰ. 연구 배경

인터넷의 보급이 확산되고 디지털화된 콘텐츠(E-Book, 인터넷 TV, Image, Video, Music 등)를 유통하는 상업적인 모델이 점차 자리를 잡아감에 따라 디지털 콘텐츠의 저작권보호 기술에 대한 필요성이 매우 중요하게 부각되고 있다.

디지털 기술의 발달로 콘텐츠의 대량 복사가 가능하고, 통신망의 발달로 아무런 제약 없이 다량의 콘텐츠 배포가 가능하게 되어 고유한 개인의 창작물이 무분별하게 도용되고 있어 디지털 컨텐츠를 제공하고 있는 업체들(CP/ISP: Contents Provider/Internet Service Provider)에게는 저작권 보호 및 불법 복제의 문제가 심각하다. 인터넷 정보통신에 대한 보안 문제와 저작권 문제가 중요한 이슈로 대두됨에 따라 콘텐츠의 판권을 보호하고 불법 복제를 방지하기 위한 기술 개발이 점점 중요시되고 있다[1].

워터마킹은 콘텐츠를 보호하기 위해 특별한 형태의 워터마크를 감추고 추출하는 모든 기술적 방법으로 초기에는 콘텐츠 저작물 자체에 은닉시키는 방법을 연구하였지만, 현재에는 마크의 인지, 강인성 제공, 삽입/검출방식, 마크의 삽입영역 등으로 분류하여 많은 기술적 변환방법을 이용한 강력한 워터마킹 기술이 개발되고 있다[2][3].

현재까지 개발된 DRM(Digital Rights Manageme-nt) 기술은 디지털 콘텐츠 전체 유통 프로세스와 암호화, 네트워크, 정보관리 등 핵심 정보기술을 결합한 「시스템 기반형」과 암호화, 워터마킹 등 요소기술을 활용한 「요소기술 기반형」을 중심으로 발전하고 있다[4].

디지털 기술이 가지는 "수정 및 복제"이란 특성 때문에 디지털 콘텐츠의 산업 발전에 많은 문제점이 발생하였다. 즉 원본 콘텐츠가 허가 없이 수정되거나 복제될 수 있으며, 인터넷을 통하여 비상업적으로 배포될 수 있으며 이로 인한 콘텐츠에 대한 소유권 문제가 발생하였다. 이것은 디지털 콘텐츠 저작권자 및 유통기업의 수입창출에 피해를 주어, 디지털 콘텐츠 산업 발전의 저해요소가 된다[5].

따라서 디지털 콘텐츠의 저작권 보호와 관리 및 산업발전을 위해 다음과 같은 요구사항이 필요하다.

① 불법복제 및 수정 방지 : 디지털 콘텐츠 불법적 복제 및 수정 등을 원천적으로 방지해야 한다.
② 접근 통제 서비스 : 인터넷 서비스는 허가된 사용자만이 서비스를 이용할 수 있어야 한다.
③ 디지털 콘텐츠 검증: 다양한 응용프로그램에서 인증된 콘텐츠만을 플레이 할 수 있는 검증 기술이 필요하다.
④ 콘텐츠 보호를 위한 새로운 기술이 필요 : 플레이어와 콘텐츠 간에 유기적인 관계를 형성하여 콘텐츠를 보호하는 기법이 필요하다.
⑤ 사용자별 콘텐츠 사용영역의 제한 : 사용자별 사용권한영역에 정책을 적용하여 콘텐츠를 제공할 수 있어야 한다.

본 논문에서는 콘텐츠 보호를 위해 필요한 요구사항을 고려하여 콘텐츠 유통 및 배포를 위한 사용자 인증키를 생성하여 인증된 사용자만이 콘텐츠를 사용할 수 있도록 인증 시스템을 구축하고, 각각의 사용자별 콘텐츠 사용권한 영역 내에서만 플레이가 가능하도록 정책을 적용하였다. 그리고 무단으로 불법 복제된 콘텐츠를 보호하기 위한 기법으로 콘텐츠와 플레이어간에 유기적인 정책을 적용하여 인증된 사용자 및 콘텐츠 암호화를 제공하여 안전한 콘텐츠 보호를 제공한다.

Ⅱ. 디지털 콘텐츠 보호 기술

1. 디지털 콘텐츠 보호 기술 요구사항

DRM은 디지털 콘텐츠가 생성될 때부터 배포, 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[11][12].

〈표 1〉은 콘텐츠 보호를 위해 필요한 기술요소이다.

표 1. 콘텐츠 보호 기술요소

항 목	설 명
Contents Encryption	• 암호화 알고리즘을 이용하여 콘텐츠를 암호화하여 사용자에게 안전하게 전달하고 재생 시 복호되어 제공 • 복호키는 인증된 사용자에게만 제공
Usage Rule	• 사용자의 요구 및 권한에 의한 콘텐츠 사용제한, Contents Provider의 다양한 마케팅 전략에 의해 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	• 디지털 콘텐츠의 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

2. 기존 디지털 콘텐츠 관리 기술

DRM 기반의 디지털 콘텐츠 관리기술은 사용자를 인증하고, 인증된 사용자만이 CP/ISP와 협약된 콘텐츠 제어범위 내에서 이용을 허용하는 기술이다. (그림 1)은 공개키 기반의 디지털 콘텐츠 관리기술을 보인다.

디지털 콘텐츠는 CP/ISP에 의해 사용자에게 제공된다. 콘텐츠를 필요로 하는 사용자는 인증기관에 의해 신분을 확인하는 인증서를 요청하여 발급 받는다[7].

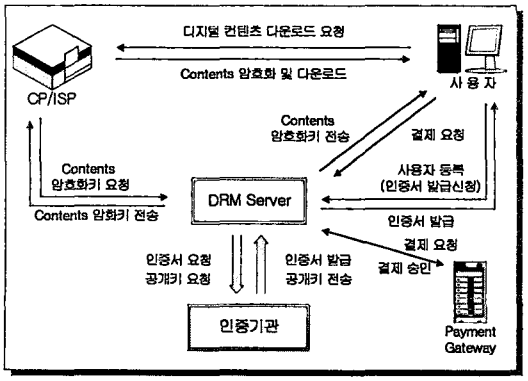

그림 1. 공개키 기반의 콘텐츠 관리

인터넷에서 제공되는 디지털 콘텐츠는 사용자 인증을 위해 인증기관에 의해 신분 확인 후 DRM 서버에 의해 콘텐츠가 보호되어 사용자에게 제공되는 유통구조를 가진다.

현재 사용되어지는 콘텐츠 서비스는 〈그림 2〉와 같은 유통구조를 가진다.

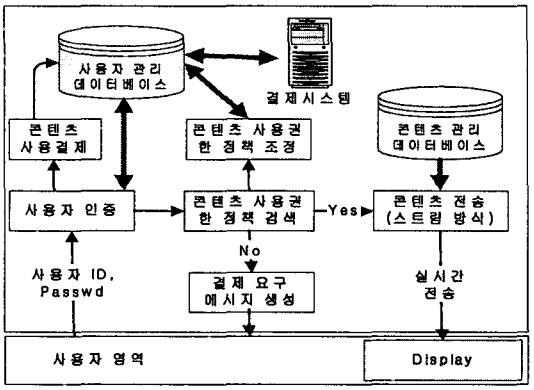

그림 2. 기존의 스트림 방식을 이용한 콘텐츠 유통 구조

사용자에게 실시간의 특성을 가진 스트림 방식을 이용한 콘텐츠가 제공되며, 스트림 방식을 이용한 콘텐츠의 제공은 네트워크의 트래픽에 영향을 받게 된다. 트래픽이 많은 네트워크 환경에서는 사용자에게 끊김이 발생하는 콘텐츠를 제공하여 원활한 콘텐츠를 제공하지 못하는 구조를 갖는다. 그러므로 기존 스트림 방식을 이용한 콘텐츠 관리는 멀티미디어와 같은 많은 정보를 가진 콘텐츠에는 적합하지 않은 단점이 있다.

또한 디지털 콘텐츠 보호를 위한 기술로, 관용암호화 방식을 이용하여 콘텐츠 서비스는 한번의 신분확인을 통해 모든 권한을 주는 결과를 초래하고 불법복제 및 허가되지 않은 사용자의 접근, 불법수정 등의 문제를 일으킬 수 있다.

그러므로 본 논문에서 제안한 시스템은 웹 서버에서 제공한 스트림 방식과 관용화 암호화 방식을 이용한 콘텐츠 서비스의 문제점을 해결 할 수 있는 콘텐츠 전용 재생기를 이용하여 디지털 콘텐츠를 안전하게 보호하고 사용자별 사용권한 영역에 따라 다양한 서비스를 지원한다.

III. 제안 디지털 콘텐츠 관리시스템 설계

1. 시스템 구성

기존 멀티미디어 컨텐츠의 위·변조 행위에 대한 방지기술로는 암호 알고리즘을 적용해 암호를 풀 수 있는 사용자에게만 그 컨텐츠를 공개하고 있는데, 암호 알고리즘에 따라 훌륭한 보안체계를 구현할 수는 있지만, 인터넷 환경에서 사용하기에는 한계가 있다. 즉, 그 사용자의 범위를 제한하며 컨텐츠를 사용할 때마다 매번 암호를 입력하는 방식이 있으나 해독된 후에는 아무런 제재 없이 위·변조, 재사용 및 재전송이 가능하다는 점에서 그 효용성에 문제점이 제기되어 왔다.

제안 시스템은 디지털 콘텐츠 자체를 보호하려는 방식에서 전용 재생기를 이용하여 콘텐츠를 보호하는데 중점을 두어 설계하였다. 관리시스템은 콘텐츠를 제공하는 CP/ISP와 콘텐츠를 이용하고자 하는 사용자로 나눌 수 있다. 즉 콘텐츠를 제공하고 총괄 관리하는 콘텐츠 관리시스템과 콘텐츠 전용재생기와의 정보교환을 통해 디지털 콘텐츠를 보호한다.

전용 재생기는 콘텐츠의 사용자 권한범위, 사용기간 등의 콘텐츠 보호와 관리를 위해 콘텐츠 정보를 가진다. 콘텐츠 보호 및 관리를 위한 정보는 관리시스템에서 암호화되어 전송되어야 하므로 암호 키를 전용 재생기에서 생성하여 공개키로 암호화하고 관리시스템에 전송한다. 관리시스템은 개인키로 복호화하고 회원의 사용범위 및 권한을 회원의 전용 재생기에서 전송된 키로 암호화하여 전송한다. 이 암호화 정보는 전용 재생기에서 복호되어 콘텐츠 등록정보를 이용해 관리되고 제어된다.

2. 디지털 콘텐츠 관리 시스템

사용자와 CP/ISP 간에 원활한 인터페이스는 공개키 기반으로 정보가 보호된다. 〈그림 3〉은 사용자 등록과 콘텐츠 구매, 결제가 이루어진 후 발생하는 콘텐츠 배포와 플레이를 위한 관리 정책을 보여준다. 사용자는 다운로드 받은 콘텐츠 전용 재생기에 의해 발생한 Random Key와 Player ID, User ID, Password를 통합하여 공개키로 암호화하여 공급자에게 정보를 전송한다.

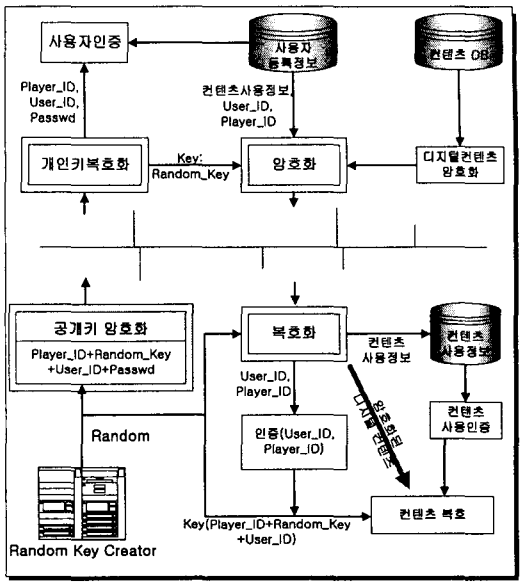

그림 3. 디지털 콘텐츠 관리 정책 구조도

'Player_ID + Random_Key + User_ID + Passwd'는 CP/ISP에 의해 개인키로 복호되고 Player ID와 User ID는 사용자 인증을 위한 정보이다. 즉 사용자 등록정보와 실제 사용자에게 배포되어 등록된 전용 재생기 ID를 비교하여 인증이 이루어지고 인증된 사용자가 구입한 콘텐츠를 제공한다. 결제가 이루어진 콘텐츠는 암호화되어 사용자에게 전송된다. 사용권한 정책과 콘텐츠 필터 암호 정보는 User ID, Player ID와 함께 Random Key로 암호화되어 사용자에게 전송한다. 즉 사용자가 CP/ISP에게 전송하는 정보는 공개키 기반인 반면에 디지털 콘텐츠 보호를 위한 암호화는 관용암호화 방식으로 이루어진다.

사용자에게 전송된 암호화된 디지털 콘텐츠와 사용자 정보는 난수 키에 의해 보호된다. 복호된 User ID와 Player ID는 사용자가 요청한 정보인지 확인을 위한 인증 정보를 제공한다. 또한 암호화된 콘텐츠 사용 정책 정보는 콘텐츠 플레이 제어를 위한 정보이다. 안전하게 전송되고 인증된 사용자는 디지털 콘텐츠를 사용할 수 있다.

3. 디지털 콘텐츠 전용 플레이어

사용자의 디지털 콘텐츠는 〈그림 4〉과 같이 CP/ISP에서 제공하는 관리시스템의 제어에 의해 사용자의 디지털 콘텐츠는 보호되고 콘텐츠 전용 재생기에 의해 디스플레이 된다. CP/ISP로부터 제공되는 콘텐츠 전용 재생기는 사용자 등록과 디지털 콘텐츠 구매에 의해 제공되는 플레이어이다.

전용 재생기는 사용권한정보를 근거로 콘텐츠를 제어한다. 또한 콘텐츠 복호 필터 정보와 User ID, Player ID를 기반으로 사용인증과 콘텐츠 필터 복호에 의해 사용자에게 디스플레이 된다. <그림 4>는 디지털 콘텐츠 보호를 위한 전용 재생기 모듈 구조이다.

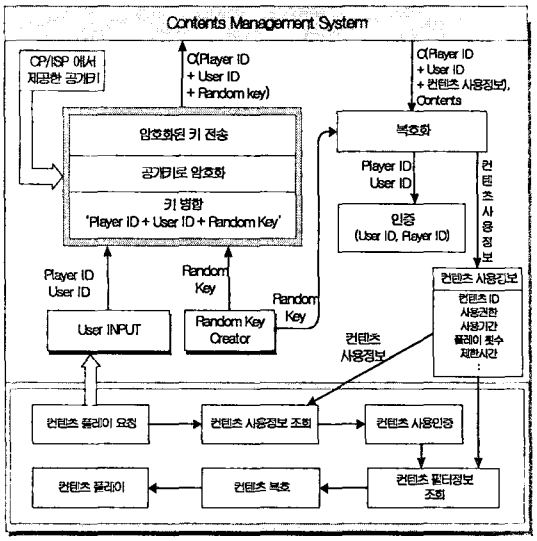

그림 4. 콘텐츠 전용 재생기 모듈

4. 디지털 콘텐츠 보호 알고리즘

원영상 정보에 임의의 필터를 적용하여 콘텐츠는 왜곡된 정보를 가지며 복호시에는 왜곡된 필터 정보가 적용되어 복호되는 기본 알고리즘이 적용된다.

4.1 콘텐츠 Encoding

소스 파일을 읽어 들이는 형태를 정의한 루틴으로 파일의 형태를 크게 세 가지로 구분하여 데이터를 읽어 들인다. 즉 R, G, B 형태의 파일을 읽는 것이 아니라 압축의 효과를 가져오는 Y, Cb, Cr의 형태로 파라미터 파일에 설정된 값에 의해 각각의 파일이 설정된다. YUV 표현은 사람의 시각 특성상 색차신호보다 밝기신호에 더 민감하기 때문에 밝기 신호와 색차신호를 분리하면 영상 압축시 효율성을 발휘한다. 실제 RGB 표현은 영상의 압축에 불리하며 YUV 표현을 사용하면 발기 신호인 Y(luminance)와 색차신호인 U, V(chrominance)로 분리되기 때문에 압축이 용이하다. 이런 특성을 가진 YUV를 이용하여 각각의 정보에 필터를 적용하여 원영상 정보를 왜곡시켜 콘텐츠를 보호한다. 필터 정보는 난수 키에 의해 생성된 키이다. <그림 5>는 YUV 정보에 필터를 적용 시켜 정보를 왜곡하는 모듈의 기능이다.

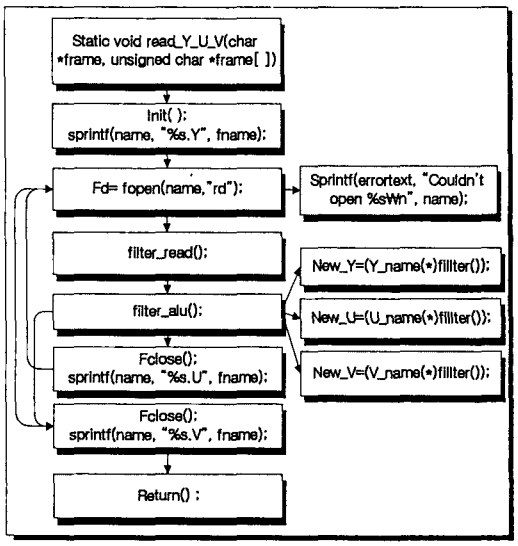

그림 5. YUV 필터 적용 모듈

프레임 처리 루틴에 의해 호출된 필터 적용 모듈은 적용될 콘텐츠 YUV를 각각 불러 들여 필터 정보를 적용한다. 적용된 YUV는 필터 키로 왜곡된 정보를 복구할 수 있다.

또한 DCT 계수는 2차원 값이므로 1차원 값으로 변환하여 부호화해야 한다. 이때 저주파는 저주파끼리 고주파는 고주파끼리 묶어 놓는 것이 압축효율을 증가시킨다. 이 방법을 스캐닝이라 하고 이것을 이용하여 색차정보와 함께 소실량을 적용한다. 소실량은 사용 권한정책에 준한다.

콘텐츠에 적용되는 콘텐츠 필터는 지수함수를 이용한 난수를 이용한다. 필터 정보는 콘텐츠 등록 시 적용되어 사용자에게 제공되며, 난수에 의해 발생된 필터 정보는 콘텐츠 필터 테이블에 저장, 관리되고 사용자 요청 시 사용자로부터 전송된 난수 키에 의해 DES로 암호화되어 전송된다.

4.2 콘텐츠 Decoding

프레임 복호는 한 장의 픽처 안에 매크로 블록의 개수만큼 반복을 통하여 프레임을 복호화 하는 루틴이다.

각 프레임의 매크로 블록의 수와 영상의 크기, 한 영상에 대한 버퍼 크기, DCT의 초기화 과정 이후 한 프레임에 대한 헤더를 복호화한 후 픽처 복호화 루틴을 실행한다. 다음으로 현재 픽처의 모든 매크로 블록을 복호화 한다. 매크로 블록의 복호를 위하여 현재 프레임에서 슬라이스를 읽어 들이고 부호기에서 설정한 각각의 매크로 블록 형태를 파악하여 각 블록에 대한 움직임 벡터가 존재 하는지를 판단한다. 각 블록에 대한 복호화를 수행하면서 움직임 벡터가 존재하면 움직임 보상 작업에 들어가고, 움직임 벡터가 존재하지

않으면 바로 IDCT를 수행하며, IDCT를 수행하면서 데이터 값의 범위를 조사하여, 움직임 보상 이후에 발생하는 데이터의 예측 값을 add_block()를 통하여 수행함으로써 실질적인 영상을 만든다. 프레임의 소실은 영상 복원 시 플레이에서 정책에 따라 소실여부와 소실 양을 결정하여 제어된다. 프레임 복원 시 필터 정보와 원영상 복원은 (그림 6)과 같다.

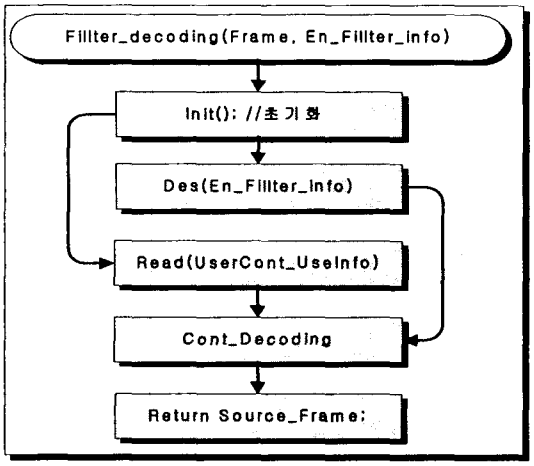

그림 6. 필터 Decoding

필터가 적용된 프레임과 필터 정보를 입력 데이터로 받아 들여 암호화된 Filter_info를 복호화 한다. 복호된 필터 정보로 프레임에 적용하여 원영상을 추출한다. 원영상 추출 과정에 사용자 사용권한 정책에 기준하여 영상의 복원 정보를 결정하여 프레임을 출력한다. 이렇게 출력된 프레임들이 모여 하나의 영상을 만든다.

Ⅳ. 디지털 콘텐츠 보호 시스템 구현 및 분석 평가

성능 테스트 시나리오 디지털 콘텐츠 보호의 요구사항에 따라 다음 항목을 중심으로 실험하였다.

(1) 본 시스템에서 제공하는 디지털 콘텐츠가 범용 플레이어에서 보호되는가?

(2) 디지털 콘텐츠 사용 권한 정책에 의한 소실량과 사용 권한 제어가 가능한가?

(3) 시스템 운영에 필요한 인증처리가 네트워크 트래픽에 미치는 영향은 어떠한가?

1. 디지털 콘텐츠 보호

일반 미디어 플레이어에서 본 시스템에서 제공하는 콘텐츠를 플레이한 결과를 〈그림 7〉에서 보인다. 플레이어는 Windows Media Player 9를 이용하였다.

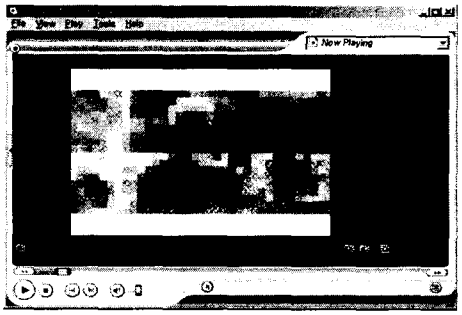

그림 7. Windows Media Player Execute

콘텐츠가 필터링 된 결과로 Windows Media Player에서는 식별할 수 없는 콘텐츠를 제공한다.

2. 디지털 콘텐츠 사용제한 정책

콘텐츠 사용이 인증된 사용자는 사용권한내에서 사용이 가능하다. 〈그림 8〉은 콘텐츠 사용 권한 내에서 사용 시 디스플레이 화면이다. 콘텐츠 사용권한 획득 시 정상적으로 디스플레이 되는 화면이다. 〈그림 9〉와 〈그림 10〉은 사용권한 횟수가 초과 될수록 콘텐츠의 왜곡 현상이 심해지는 디스플레이를 보인다. 사용권한내에서의 콘텐츠 사용은 정상적인 콘텐츠가 제공되고 만기된 콘텐츠는 사용횟수에 따라 디스플레이 화면이 왜곡된 결과를 가진다.

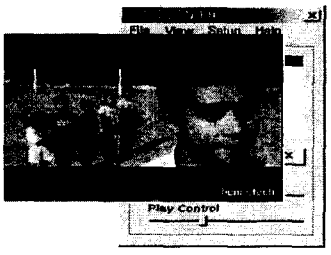

그림 8. 콘텐츠 사용권한내 플레이 화면

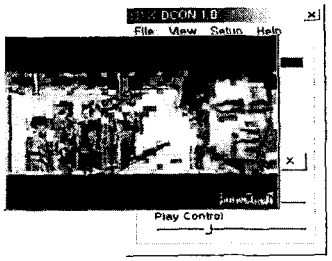

그림 9. 사용권한 1회 초과 플레이화면

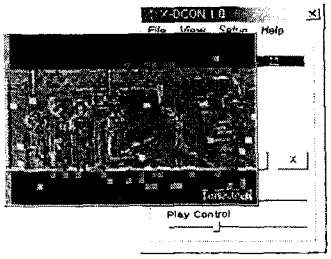

그림 10. 사용권한 4회 초과 플레이 화면

3. 사용자 인증 네트워크 트래픽

〈그림 11〉은 콘텐츠 사용권한 획득을 위해 관리서버와 전용재생기간의 상호 인터페이스가 네트워크에 미치는 영향을 조사하기 위한 네트워크 트래픽 화면이다.

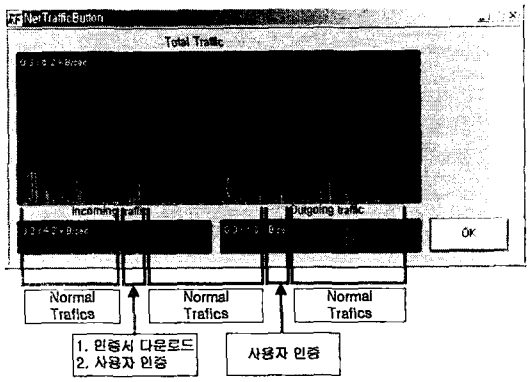

그림 11. 네트워크 트래픽

관리서버와 재생기간 상호 인증을 위한 네트워크 트래픽은 암호화된 콘텐츠 필터 정보가 발급되는 과정에서 Normal 트래픽의 2.0KB/Sec에서 4.3KB/Sec로 순간적인 네트워크 트래픽을 발생시키므로 콘텐츠 사용을 위한 사용자 인증 및 콘텐츠 필터 정보 전송은 Normal 트래픽과 별다른 트래픽을 발생하지 않았다.

4. 성능 시험 결과

성능 테스트 시나리오에 의한 시스템 실험 결과는 다음과 같은 결과를 얻었다.

① 콘텐츠는 필터링되어 사용자에게 제공되고, 콘텐츠 복호 시 필터 정보를 사용자에게 전송된다. 필터 정보는 암호화되어 사용자에게 제공되므로 안전성이 보장된다.

② 사용 권한 정책에 의한 콘텐츠 사용 권한 초과 시에 콘텐츠 소실이 이루어지므로 콘텐츠의 사용권한 정책에 대한 제어와 관리가 원활하게 이루어진다.

③ 네트워크를 통한 서버와 클라이언트간에 인터페이스가 적으므로 네트워크 트래픽에 대한 속도의 저하의 문제가 발생하지 않는다.

④ ActiveX를 이용한 서비스는 네트워크의 속도에 많은 제약을 받아 현재로써는 콘텐츠 제공이 끊김이 발생하는 취약점을 실시간 사용자 인증만으로 On/Off Line 으로 제공된 콘텐츠를 원활하게 사용할 수 있다.

V. 결 론

본 논문에서는 네트워크를 통한 사용자 인증과 사용 횟수에 따라 콘텐츠가 소실되는 기술, 콘텐츠 자체를 암호화하여 제공함으로써 불법복제의 위험성을 제거하여 안전하게 콘텐츠를 보호하는 시스템을 개발하였다.

제안 시스템은 기술적인 측면에서 사용자 관리와 콘텐츠 관리 영역으로 구분할 수 있다. 사용자 관리는 사용자와 콘텐츠인증으로 사용권한 인증을 제공하고, 콘텐츠 관리는 범용 콘텐츠에 콘텐츠 고유 필터를 적용하여 암호화된 콘텐츠를 사용자에게 제공한다.

콘텐츠는 일반인 누구나 접할 수 있는 특성을 가진다. 그러나 본 시스템은 디지털 콘텐츠 전용 재생기에서 인증된 사용자만이 디스플레이가 가능하도록 암호화되어 제공된다. 콘텐츠 자체에 콘텐츠 필터 정보가 사용자 인증키로 암호화되어 인증된 사용자만이 콘텐츠를 사용할 수 있도록 개발하여 무분별한 사용을 방지한다. 또한 콘텐츠 필터 정보를 제어하여 사용권한에 따라 사용할 수 있는 횟수를 제안할 수 있도록 하였다.

본 연구로 콘텐츠의 무분별한 유통과 불법복제에 의한 콘텐츠 시장의 위험요소를 해결하고, 콘텐츠 시장에 안전하고 경제적인 활성화가 이루어질 것으로 기대된다.

참고문헌

[1] 전종민, 최영철, 박상준, 박성준, "DRM 기술 및 제품 동향 분석", 정보보학회지, 제11권, 제5호, pp.26~34. 2001.10.

[2] 정사라, 석종원, 홍진우, "디지털 컨텐츠의 저작권 관리를 위한 워터마킹 기술", 전자통신동향분석, 제16권, 제4호, 2001.8.

[3] 김경순, 임재혁, 원치선, "MPEG 동영상의 실시간 워터마킹 기법" 정보보호학회지, 제15권, 제1호, 2001.

[4] 이창열, "DRM 기술", 정보보호학회지, 제12권, 제1호, pp. 1~10, 2002.2.

[5] 원치선, "디지털 영상의 저작권 보호", 정보과학지, 제15권, 제12호, pp. 22-27, 1997.

[6] Frank Hartung, Bemd Girod, "Digital Watermarking of MPEG-2 Coded Video in the Bistream Domain", Proceedings International Conference on Acoustics, Speech, and Signal Processing (ICASSP97), Vol. 4, pp.2621-2624, Munich, April. 1997.

[7] 조용주, 안상우, 홍진우, 김진웅, "mpeg-2/4 IPMP 기술을 이용한 콘텐츠 관리 및 보호 시스템", Telecommunications Review, 제12권 5호, 2002.10.

[8] "알기 쉬운 MPEG-2 " 이호석, 김준기 홍릉과학출판사 2002.2.

[9] MPEG Requirements Group, "MPEG-21 Overview", Editors : J.bormans and K.Hill, ISO/IEC JTC1/SC29/WG11 N4511, Pattaya, Thailand, December 2001.

[10] MPEG Requirements Group, : MPEG-21 Requirements, V.1", ISO/IEC JTC1/SC29/WG11 N4700, FairFax, U.S.A May 2002.

[11] 이형우, "안전한 컨텐츠 유통을 위한 방안 연구", 정보보호학회지, 제12권, 제1호, 2002.2.

[12] 강호갑, "DRM을 이용한 컨텐츠 불법방지사용자시스템 구축 방안", KIEC, 정기간행물, 2001.3.

[13] Ji Ming, Craig A Schultz, "Information technology Coding of moving picture and audio : MPEG-4 IPMP Extension Reference Software Architecture based on IM1, 2002.

[14] Renato Iannella, "Digital Rights Management Architectures", DOLib Magazine, Vol. 7, No. 6, June 2001.

저 자 소 개

고 병 수

2000 호남대학교 컴퓨터공학과 (공학석사)

현 재 대전대학교 컴퓨터공학과 (박사수료)

〈관심분야〉 Secure OS, PKI 응용

장 재 혁

2002 대전대학교 컴퓨터공학과 (공학석사)

현 재 대전대학교 컴퓨터공학과 (박사과정)

〈관심분야〉 DRM, PKI

최 용 락

1989 중앙대학교 전자계산학과 (박사)

1982. 3 ~ 1986. 1 한국전자통신연구원 선임연구원

현 재 대전대 컴퓨터공학부 교수

〈관심분야〉 컴퓨터통신보안, 컴퓨터 포렌식스, DRM