공개키 기반의 프레임 필터 정보를 이용한 디지털 콘텐츠 보호 시스템☆

The Protection System of Digital Contents using a Frame Filter Information based on Public Key

고 병 수* 장 재 혁** 강 석 주** 최 용 락***
Byoung-Soo Koh Jae-Hyuk Jang Seok-Jue Kang Yong-Rak Choi

요 약

인터넷의 발달은 디지털 콘텐츠 시장의 활성화를 일으키는 가장 중요한 요소이다. 인터넷을 이용한 콘텐츠의 보급은 사용자에게 편리성과 효율성, 유용성을 제공한다. 그러나 콘텐츠의 불법복제와 무분별한 사용은 콘텐츠 시장을 위축시키는 장애요인으로 작용한다. 최근 인터넷을 이용한 콘텐츠 불법유통에 저작자와 공급자, 소비자간에 갈등이 유발되고 있으며 법적 소송에 이르고 있다. 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 불법도용의 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 and gives the convenience, efficiency and usefulness to the users. However the Digital Contents Market could be shrunk by an illegal reprinting and imprudent using. As a result, recently we can see that using the contents illegally through Internet makes the troubles between providers and customers and finally they are at law. 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 : Digital contents Protection / Watermarking / DRM / PKI

1. 서 론

최근 유무선 인터넷 및 네트워크 통신기술의 발전에 따른 디지털 콘텐츠의 제작과 유통의 시장 규모가 광범위하게 발전되고 있으나, 콘텐츠 불법복제 및 저작권보호에 매우 취약한 특성이 있으므로 이에 따른 저작권 침해현상이 심각한 상황에 이르고 있다.

디지털 기술의 발달로 콘텐츠의 대량 복사가 가능하고, 통신망의 발달로 아무런 제약 없이 다량의 콘텐츠 배포가 가능하게 되어 고유한 개인의 창작물이 무분별하게 도용되고 있다. 실제로 인터넷상에서 MP3 파일 또는 동영상 데이터 서비스를 제공하고 있는 업체들(CP/ISP : Contents Provider/Internet Service Provider)에게는 저작권 보호 및 불법 복제

* 정 회 원 : 대전대학교 컴퓨터공학과 대학원
kbs@zeus.dju.ac.kr(제1저자)
** 준 회 원 : 대전대학교 컴퓨터공학과 대학원
jhjang@zeus.dju.ac.kr(공동저자)
*** 종신회원 : 대전대학교 컴퓨터공학부 교수
yrchoi@dju.ac.kr(공동저자)
☆ 본 연구는 과학기술부 지역협력연구센터 (R12-2003-004-00005-0)지원으로 수행되었음.

의 문제가 심각하다. 인터넷 정보 통신에 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 워터마크(저작권 정보, 로고, 인감, 인증번호 등)를 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 Management) 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. DRM은 21세기 신산업으로 각광을 받고 있는 디지털 콘텐츠 산업의 기반을 구축하는데 필수적인 디지털 콘텐츠의 저작권보호 및 유통 인프라 시스템을 구축하는데 필수적인 기술이다[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 위해서는 불법복제 및 수정 방지기술, 접근 통제 서비스, 디지털 컨텐츠 검증 기술, 사용자별 콘텐츠 사용영역의 제한등이 필요하다.

본 연구에서는 콘텐츠 보호를 위해 필요한 요구사항을 고려하여 콘텐츠 유통 및 배포를 위한 사용자 인증키를 생성하여 인증된 사용자만이 콘텐츠를 사용할 수 있도록 인증시스템을 구축하고, 각각의 사용자별 콘텐츠 사용권한 영역내에서만 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.

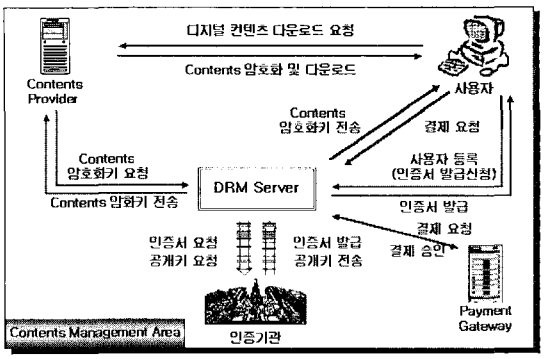
2. 디지털 콘텐츠 보호 기술

DRM은 다양한 채널을 통해 유통되는 각종 디지털 콘텐츠 서비스의 유료화를 가능하게 하는 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[6][7].

디지털 워터마크는 네트워크상에서 사용 가능한 상태로 널리 분포, 유통될 수 있는 멀티미디어 데이터 및 출판물과 같이 지적 재산권 보호 대상 성격을 지니는 자료에 대해 원 데이터에 권리자 및 인증과 같은 추가적인 정보를 삽입하여 데이터에 대한 지적재산을 보호하기 위한 기법이다. 워터마크 기술은 CP서버로부터 사용자에게 디지털 콘텐츠 데이터를 제3자가 알아볼 수 없도록 암호화하는 Front-End 기술과는 달리 저작권을 확증해주는 Back-end 기술이다.

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

DRM 기반의 디지털 콘텐츠 관리기술은 사용자를 인증하고, 인증된 사용자만이 CP/ISP와 협약된 콘텐츠 제어범위 내에서 이용을 허용하는 기술이다. 그림 1은 공개키 기반의 디지털 콘텐츠 관리기술을 보인다. 디지털 콘텐츠는 CP/ISP에 의해 사용자에게 제공된다. 콘텐츠를 필요로 하는



〈그림 1〉 공개키 기반의 콘텐츠 관리

사용자는 인증기관에 의해 신분을 확인하는 인증서를 요청하여 발급 받는다[7].

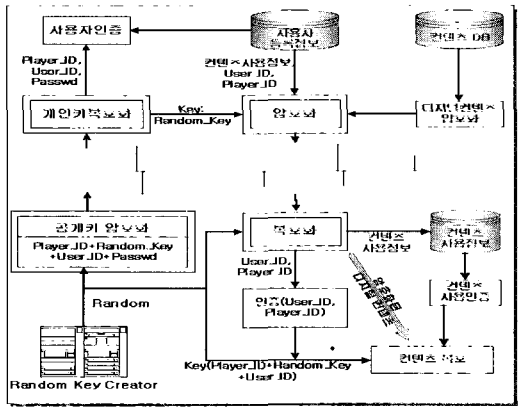
인증서를 발급 받은 사용자만이 디지털 콘텐츠를 이용할 수 있는 자격을 갖추고, CP/ISP에서 제공하는 콘텐츠를 사용할 수 있다. 다운로드 및 사용권한을 획득하기 위해서는 개인 인증서를 통해 신분 확인 후 결제처리가 이루어진다.

그러나 디지털 콘텐츠 보호를 위한 기술로 관용 암호화 방식을 이용하여 키 교환을 통해 콘텐츠가 제공된다. 콘텐츠는 한번의 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 디지털 콘텐츠를 안전하게 보호하고 사용자별 사용권한 영역에 따라 다양한 서비스를 지원한다.

3. 공개키 기반의 디지털 콘텐츠 보호시스템 설계

3.1 제안 시스템 구성

제안 시스템은 디지털 콘텐츠 자체를 보호하려는 방식에서 전용재생기를 이용하여 콘텐츠를 보호하는데 중점을 두어 설계하였다. 관리시스템은 콘텐츠를 제공하는 CP/ISP와 콘텐츠를 이용하고자 하는 사용자로 나눌 수 있다. 즉 콘텐츠를 제공하



〈그림 2〉 디지털 콘텐츠 관리 정책 구조도

고 총괄 관리하는 콘텐츠 관리시스템과 콘텐츠 전용재생기와의 정보교환을 통해 디지털 콘텐츠를 보호한다.

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

그림 2는 사용자 등록과 콘텐츠 구매, 결제가 이루어진 후 발생하는 콘텐츠 배포와 플레이를 위한 관리 정책을 보여준다. 사용자는 다운로드 받은 콘텐츠 전용재생기에 의해 발생한 Random Key와 Player ID, User ID, Password를 통합하여 공개키로 암호화하여 공급자에게 정보를 전송한다.

'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 전용재생기ID를 비교하여 인증이 이루어지고 인증된 사용자가 구입한 콘텐츠를 제공한다. 결제가 이루어진 콘텐츠는 암호화되어 사용자에게 전송

된다. 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.

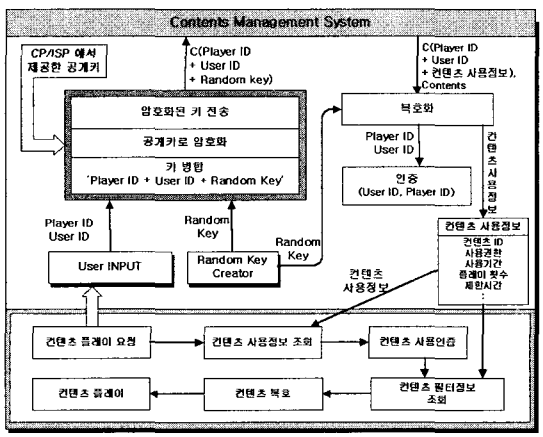
사용자에게 전송된 암호화된 디지털 콘텐츠와 사용자 정보는 난수 키에 의해 보호된다. 복호된 User ID와 Player ID는 사용자가 요청한 정보인지 확인을 위한 인증 정보를 제공한다. 또한 암호화된 콘텐츠 사용 정책 정보는 콘텐츠 플레이 제어를 위한 정보이다. 안전하게 전송되고 인증된 사용자는 디지털 콘텐츠를 사용할 수 있다.

그림 3은 디지털 콘텐츠 보호를 위한 전용재생기 모듈 구조이다.

콘텐츠 관리 시스템에서 제공되는 공개키는 사용자 인증을 위해 사용된다. 공개키로 Player ID와 User ID, User Password, Random Key가 병합되어 암호화된다. Player ID는 콘텐츠 재생을 위한

플레이어 고유 식별번호이고 사용자 식별을 위한 User ID, 사용자 인증을 위한 Password, Random Key Creator에 의해 생성된 Random Key이다.

User ID/Passwd, Player ID, Random Key는 콘텐츠 사용권한 정책과 콘텐츠 필터 정보, 사용자 인증 정보를 보호하기 위해 사용된다. 관리시스템은



〈그림 3〉 콘텐츠 전용 재생기 모듈

콘텐츠 복호에 필요한 필터 정보를 Random Key를 이용하여 암호화하여 사용자에게 전송한다. 또한 사용권한 정책정보는 관리시스템으로부터 인증확인 후 사용권한정책을 사용자에게 전송한다. 관리시스템에서 전용재생기에 전송되는 정보는 Random Key를 이용하여 DES로 암호화되어 전송되고 User ID와 Player ID는 사용자별 콘텐츠 플레이어 인증에 필요하다. 인증된 사용자는 콘텐츠 복호 필터 정보를 이용하여 실시간 복호화 됨으로써 디스플레이 된다.

3.2 콘텐츠 Encoding

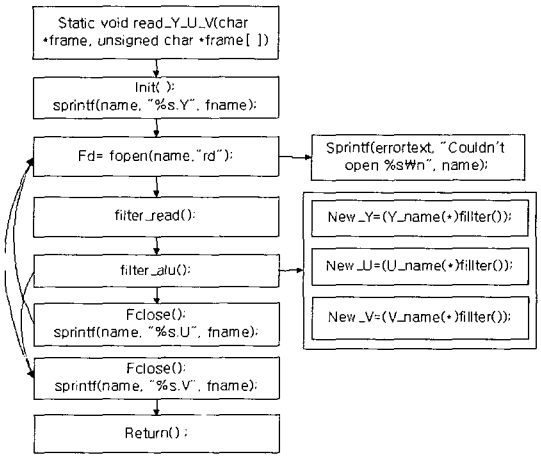
소스 파일을 읽어들이는 형태를 정의한 루틴으로 파일의 형태를 크게 세 가지로 구분하여 데이터를 읽어 들인다. 즉 R, G, B 형태의 파일을 읽는 것이 아니라 압축의 효과를 가져오는 Y, Cb, Cr의 형태로 파라미터 파일에 설정된 값에 의해 각각의 파일이 설정된다.

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 4는 YUV 정보에 필터를 적용 시켜 정보를 왜곡하는 모듈의 기능이다.

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

또한 DCT 계수는 2차원 값이므로 1차원 값으로 변환하여 부호화해야 한다. 이때 저주파는 저주파끼리 고주파는 고주파끼리 묶어 놓는 것이



〈그림 4〉 YUV 필터 적용 모듈

압축효율을 증가시킨다. 이 방법을 스캐닝이라하고 이것을 이용하여 색차정보와 함께 소실량을 적용한다. 소실량은 사용 권한정책에 준한다.

콘텐츠에 적용되는 콘텐츠 필터는 지수함수를 이용한 난수를 이용한다. 필터 정보는 콘텐츠 등록시 적용되어 사용자에게 제공된다. 난수에 의해 발생된 필터 정보는 콘텐츠 필터 테이블에 저장되어 관리되고 사용자 요청시 마다 사용자로부터 전송된 난수키에 의해 DES로 암호화되어 전송된다. 필터 정보 암호화 적용 모듈은 다음 과정을 거친다.

콘텐츠 암호화를 위한 알고리즘은 필터 정보와 콘텐츠 원영상 정보를 연산하여 왜곡된 정보를 이용한다. 연산은 excusive-OR 연산을 사용한다. 콘텐츠 암호화 알고리즘은 다음과 같다.

```
char Filter_encry(int random_key)
char *filter_info, *encry_filter;
char *Rand_Key;
void DES3( );
{
    itoa(random_key, Rand_Key, 64);
    fread(filter_info); // filter information read
    // filter Information encryption
    encry_filter=DES3(Rand_Key, filter_info);
    return encry_filter;
}
```

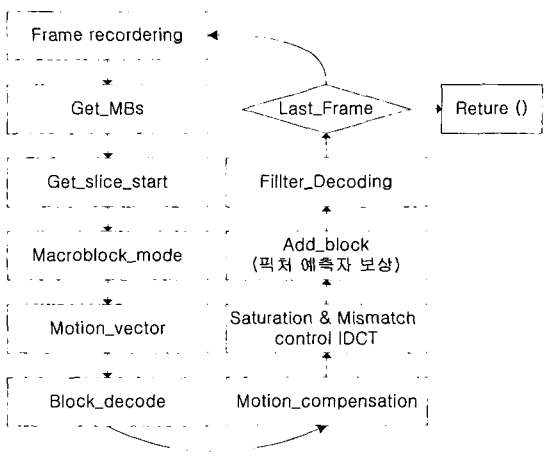
```
Contents_encry(char *filter_info, char *Y, char *U, char *V, int frame_size)
{
    for( i=0 ; i<frame_size; i++){
        Y=Y^filter_info[i];
        U=U^filter_info[i];
        V=V^filter_info[i];
    }
    return Y, U, V;
}
```

필터 정보와 콘텐츠의 색차 정보를 가진 *.Y, *.U, *.V 파일에 값을 마지막 프레임 정보까지 excusive-OR 연산하여 출력한다. 콘텐츠는 필터가 적용되어 왜곡된 정보를 가진다.

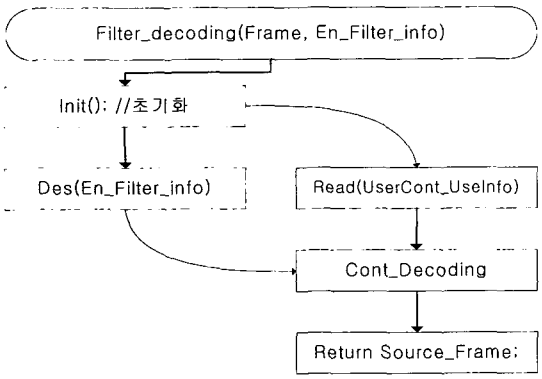
3.3 콘텐츠 Decoding

프레임 복호는 한 장의 픽처 안에 매크로 블록의 개수 만큼 반복을 통하여 프레임을 복호화 하는 루틴이다. 그림 5는 프레임 복호화 루틴이 바로 압축된 하나의 영상을 복원하는 과정이다.

각 프레임의 매크로 블록의 수와 영상의 크기, 한 영상에 대한 버퍼 크기, DCT의 초기화 과정 이후 한 프레임에 대한 헤더를 복호한다. 헤더를 복호한 후에 픽처 복호화 루틴이 실행된다. 수행되는 과정은 프레임 재순서화 과정이다. 다음으로



〈그림 5〉 프레임 복호 루틴 알고리즘



〈그림 6〉 필터 Decoding

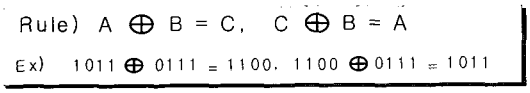
현재 픽처의 모든 매크로 블록을 복호화 한다.

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 수행한다. 또한 IDCT를 수행하면서 데이터 값의 범위를 조사하며, 움직임 보상 이후에 발생하는 데이터의 예측 값을 add_block()를 통하여 수행함으로써 실질적인 영상을 만든다.

출력되는 영상은 원 영상에 필터를 적용한 결과 값이다. 즉 부호화시 적용된 필터 정보를 복원하는 기능을 수행하는 모듈이 Filter_Decoding()이고 원 영상으로 복원된 결과 값을 출력한다.

프레임의 소실은 영상 복원시 플레이에서 정책에 따라 소실여부와 소실 양을 결정하여 제어된다. 프레임 복원시 필터 정보와 원영상 복원은 Filter_Decoding 함수에서 수행하며 그림 6과 같다.

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. 콘텐츠 정보 왜곡 정보에 적용되는 Excusive-OR 연산은 그림 7과 같은 특징을 가진다.



〈그림 7〉 Excusive-OR Rule

excusive-OR는 같은 연산을 반복하였을 경우 본래의 값이 출력된다. 이런 특징을 이용하여 'A'의 값은 콘텐츠 정보, 'B'의 값은 필터 정보, 'C'의 값은 왜곡된 콘텐츠 정보를 가진다.

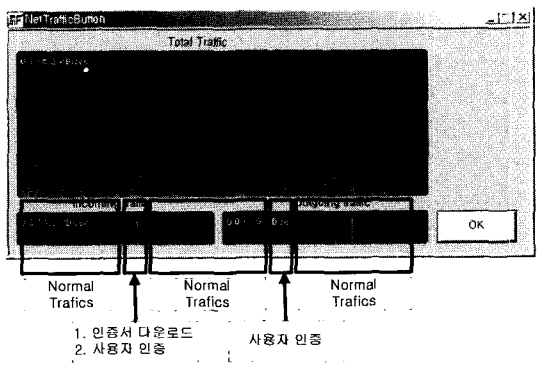
4. 보안 인증 및 컨텐츠 보호 시스템 구현

성능 테스트 시나리오는 다음 항목을 중심으로 테스트한다.

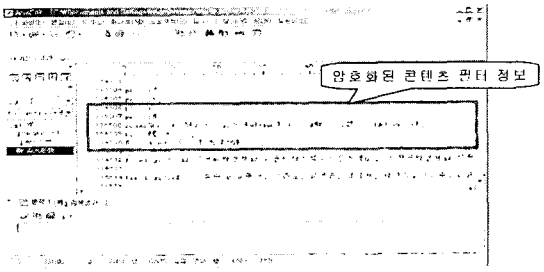
- 시스템 운영에 필요한 인증처리의 네트워크 트래픽 안정성
- 범용 플레이어에서의 디지털 컨텐츠 보호
- 디지털 콘텐츠 사용 권한 정책에 의한 소실량과 사용 권한 제어 가능성

4.1 사용자 인증 네트워크 트래픽

그림 8은 콘텐츠 사용권한 획득을 위해 관리서버와 전용재생기간의 상호 인터페이스가 네트워크에 미치는 영향을 조사하기 위한 네트워크 트



〈그림 8〉 네트워크 트래픽



〔그림 9〕 Contents filter info

래픽 화면이다.

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.

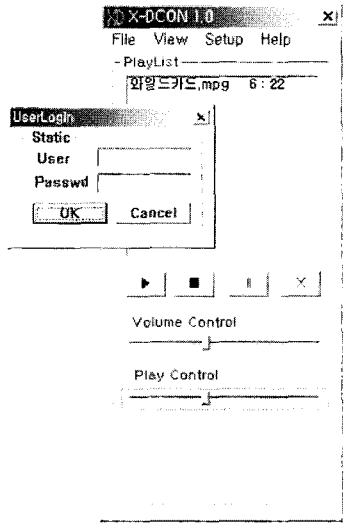
4.2 콘텐츠 보호

콘텐츠가 필터링된 결과로 Windows Media Player에서는 식별할 수 없는 콘텐츠를 제공한다. 필터 정보는 원영상 정보와 연산되는 정보로써 콘텐츠를 왜곡시키고 보호하는데 이용된다.

콘텐츠를 복호하기 위한 필터 정보와 부가 정보를 포함하는 콘텐츠 자체 정보를 그림 9에서 보인다. 원영상의 필터 정보가 암호화되어 제공되는 결과 값을 Edit Plus Editor을 이용하여 디스플레이한 화면으로 콘텐츠를 왜곡시킨 필터 정보가 암호화되어 제공된다.

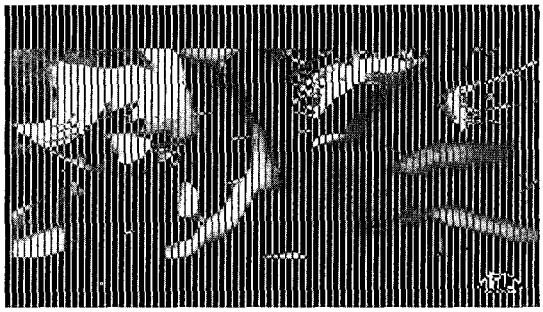
4.3 콘텐츠 사용제한 정책

콘텐츠 사용이 인증된 사용자는 사용권한내에서 사용이 가능하다. 그림 10은 콘텐츠 사용 권한 내에서 콘텐츠의 사용권한 획득 시 정상적으로 디스플레이되는 화면이다. 그림 11과 그림 12는 사용권한 횟수가 초과 될 수록 콘텐츠의 왜곡 현상이 심해지는 디스플레이를 보인다.



〔그림 10〕 콘텐츠 사용권한내 플레이 화면

〔그림 11〕 사용권한 1회 초과 플레이화면



〔그림 12〕 사용권한 4회 초과 플레이 화면

사용권한내에서의 콘텐츠 사용은 정상적인 콘텐츠가 제공되고 만기된 콘텐츠는 사용횟수에 따라 디스플레이 화면이 왜곡된 결과를 가진다.

4.4 테스트 결과

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

- 콘텐츠는 필터링하여 사용자에게 제공되고, 콘텐츠 복호시 필터 정보를 사용자에게 전송된다. 필터 정보는 암호화하여 사용자에게 제공되므로 안전성이 보장된다.
- 사용 권한 정책에 의한 콘텐츠 사용 권한 초과시에 콘텐츠 소실이 이루어지므로 콘텐츠의 사용권한 정책에 대한 제어와 관리가 원활하게 이루어진다.
- 네트워크를 통한 서버와 클라이언트간에 인터페이스가 적으므로 네트워크 트래픽에 대한 속도의 저하의 문제가 발생하지 않는다.
- ActiveX를 이용한 서비스는 네트워크의 속도에 많은 제약을 받음으로써 콘텐츠를 제공함에 끊김이 발생하는 취약점을 실시간 사용자 인증만으로 보완하여 콘텐츠를 원활하게 사용할 수 있다.

5. 결 론

본 논문에서는 디지털 콘텐츠 시장의 활성화를 위해 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 암호화하여 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 디지털 콘텐츠의 개발에 의한 새로운 콘텐츠 시장의 발전 방향을 제시하며 콘텐츠 시장에 활성화가 경제적인 측면에 이루어질 것으로 기대된다.

참 고 문 헌

[1] 전종민, 최영철, 박상준, 박성준, "DRM 기술 및 제품 동향 분석", 한국정보보호학회지, 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" 한국정보보호학회지, 제15권, 제1호, 2001.

[4] 이창열, "DRM 기술", 한국정보보호학회지, 제12권, 제1호, pp. 1~10, 2002. 2.

[5] 원치선, "디지털 영상의 저작권 보호", 한국정보과학지, 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] MPEG Requirements Group, "MPEG-21 Overview", Editors:J.bormans and K.Hill, ISO/IECJTC1/SC29/ WG11 N4511, Pattaya, Thailand, December 2001.

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

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

[11] Renato Iannella, "Digital Rights Management Architectures", D0Lib Magazine, Vol. 7, No. 6, June 2001.

◐ 저 자 소 개 ◑

고 병 수
2002년 호남대학교 컴퓨터공학과(학사)
2000년 호남대학교 컴퓨터공학과(석사)
2000년~현재 : 대전대학교 컴퓨터공학과(박사수료)
관심분야 : Secure OS, PKI 응용
E-mail : kbs@zeus.dju.ac.kr

장 재 혁
2002년 대전대학교 컴퓨터공학과(학사)
2002년 대전대학교 컴퓨터공학과(석사)
2002년~현재 : 대전대학교 컴퓨터공학과(박사과정)
관심분야 : DRM, PKI
E-mail : jhjang@zeus.dju.ac.kr

강 석 주
1995년 대전대학교 컴퓨터공학과 졸업(석사)
2003년 대전대학교 컴퓨터공학과 (박사수료)
2000년~현재 : 프로그램심의조정위원회 정보사업팀
관심분야 : 지적재산권, DRM
E-mail : sjkang@pdmc.or.kr

최 용 락
1989년 중앙대학교 전자계산학과(박사)
1982년~1986년 한국전자통신연구원 선임연구원
2000년~2002년 한국인터넷정보학회 기획이사
1986년~현재 : 대전대학교 컴퓨터공학부 교수
관심분야 : 컴퓨터통신보안, 컴퓨터 포렌식스, DRM
E-mail : yrchoi@dju.ac.kr