범용적인 DRM 보호를 위한 디지털 콘텐츠 순열 재조합 기법 설계

정병옥*, 김지영*, 최용락*

*대전대학교 컴퓨터공학과

A Design of Digital Contents Permutation Mixing Techniques for Multi-Purpose DRM

Byung-Ok Jeong* , Ji-Young Kim*, Yong-Rak Choi*

*Dept of Computer Engineering, Daejeon University.

요 약

기존의 DRM 보호기법은 특정 콘텐츠 포맷에 일부 제한적인 보호방식의 특성이 있기 때문에 현재 모든 디지털 콘텐츠에 대해서 범용적으로 DRM 보호기법을 적용할 수 없는 문제점이 있으므로, 아직도 많은 종류의 디지털 콘텐츠는 DRM 보호기능을 제공받지 못하고 있다. 또한, 기존의 DRM 보호기법은 암호화 알고리즘을 기반으로 많은 양의 데이터에 대해서 암/복호화를 수행하기 때문에 속도가 많이 소요되는 단점이 있다.

본 논문에서는 범용적인 DRM 보호를 위해 콘텐츠 헤더의 부분 암호화 방식과 분할된 콘텐츠에 대한 순열 재조합을 이용한 방법으로 모든 디지털 콘텐츠에 대해서 범용적으로 DRM 보호기능을 제공하는 기법을 제안하였다. 또한 이 기법은 콘텐츠의 암/복호화 수행 속도를 향상 시키고 동시에 기존의 보안성은 유지하는 기능을 포함하고 있으므로 다양한 형식의 디지털 콘텐츠에 대하여 유연하게 적용이 가능하며, 다양한 비즈니스 환경에 확장성 있는 통합 가능하다.

I. 서론

디지털 저작권 관리(Digital Rights Management) 기술은 디지털 콘텐츠를 저작권자와 제공자로부터 고객에게 정확하고 안전하게 전달하며, 디지털 콘텐츠의 라이프 사이클에 관련된 모든 주체들의 권리를 보호하는 것이 가장 큰 목적이며, 고객이 콘텐츠를 사용하는 것에 다양한 권한제어, 콘텐츠 유통 모델을 지원 하면서, 불법적인 유통 및 재배포하는 것을 방지하는 기술이다[1][2].

콘텐츠를 보호하기 위한 기반 기술로서는 암호화 방식이 사용되는데, 기존 DRM 솔루션들은 암호화에 사용된 비밀키를 사용하여 사용자가 파일을 다운로드 할 때 암호화를 수행하므로 많은 시간이 소요된다. 또한, 복호화를 수행하는 경우에도 대용량의 저작물인 경우 전체 파일에 대하여 복호화를 먼저 수행한 후에 실행을 할 수 있으므로 사용자가 실시간으로 파일을 재생해서 볼 수 없고, 콘텐츠 포맷에 대한 분석이 선행 되어야 하는 추가적인 시간이 소요되는 문제점이 있다[2][3].

기존 솔루션들은 DRM 벤더 별 고유 포맷 사용으로 콘텐츠가 상호호환성 보장이 제한적이고, 동일한 콘텐츠 포맷에 대한 DRM 솔루션이라도 벤더별로 시스템 구축방법의 차이와 콘텐츠 구성의 차이, DRM 엔진의 차이로 인해서 콘텐츠 간 상호 호환성이 보장되지 않고 있다. 따라서, 현재의 DRM은 다양한 종류의 디지털 콘텐츠 또는 다양한 환경에 동일한 DRM 보호기법을 적용하는데 한계가 있다[1][3].

본 논문에서는 표 1과 같은 요구사항을 도출하여 향상된 암/복호화 속도와 기존의 보안성을 유지하면서 현재 존재하는 모든 종류의 콘텐츠에 대하여 유연하고, 확장성 있게 보호할 수 있는 기법으로 디지털 콘텐츠 헤더의 부분 암호화와 분할된 콘텐츠의 순열 재조합 방식을 이용한 범용적인 DRM 보호기법을 제안하고 설계 하고자 한다.

요구사항	
암/복호화 속도 (Performence)	효율성
지속적보호(Parsistent Protection)	보안성
유연성(Flexibility) 통합 용이성(Seamless)	유연성 확장성

(표 1) 제안하는 기법의 요구사항 도출

II. 관련연구

2.1 기존 솔루션의 문제점

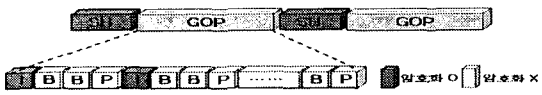
대표적인 DRM 업체인 InterTrust의 DRM 솔루션 특징은 저작물의 보호를 위해서 암호기술과 워터마킹을 사용하여 DRM 보호를 수행한다.

(그림 1) InterTrust DRM 복호화 시간

InterTrust의 DRM 시스템의 복호화는 그림 1과 같이 콘텐츠에 대한 전체 복호화가 끝난 후에 재생이 가능하므로 재생지연시간이 발생하는 문제가 있다[4]. 또한, 단일 키로만 암호화하기 때문에 키가 유출이 될 경우 더 이상 디지털 콘텐츠는 보호를 받지 못할 수 있고, 파일 전체를 암호화 하므로 암/복호화 하는데 걸리는 시간이 다른 시스템보다 오래 소요되며 재생 시 전체 복호화가 끝난 후에야 재생이 되는 문제와 지원하는 솔루션으로는 콘텐츠 종류에 따라 개별적으로 ASP-DRM, EK-DRM 등과 같이 개별 솔루션들이 존재해야만 하는 단점이 있다.

MicroSoft의 DRM 시스템은 저작물 제공자와 소비자들에게 디지털 미디어 파일을 안전하게 분배하는 종단 간(end-to-end) DRM 시스템이다. Microsoft사의 DRM 시스템의 경우는 자사의 WMV, WMA, ASF의 일부 파일 포맷만을 지원하고, 암호화 시 파일 전체를 인코딩하여 암호화하기 때문에 시간이 오래 걸리며 복호화 시에도 많은 시간이 소요되는 단점이 있다.[4]

I-Frame만은 부분 암호화 하는 DRM 시스템은 그림 2와 같이 MPEG 동영상 GOP(Group Of Picture)의 I-Frame을 대칭키를 이용하여 AES 알고리즘이나 SEED 알고리즘 중에서 하나를 선택하여 암호화하여 MPEG-2에 대한 보호 기법이다.[4]



(그림 2) I-Frame 암호화 방법

I-Frame DRM 시스템은 MPEG(Moving Picture Expert Group)데이터에서 I-Frame만을 암호화 하기 때문에 부분 암호화 방식에 속하며 이는 암호화 및 복호화 속도가 향상된다. 하지만, I-Frame을 추출하기 위해서 GOP (Group of Picture) 그룹의 모든 헤더의 내용을 읽은 다음 I-Frame의 크기를 계산하여 복호화 하는 시스템이기 때문에 모든 GOP를 읽는데 시간이 많이 소비된다. 또한, MPEG 특정 미디어 포맷에 대하여 보호하는 방식이므로 다양한 콘텐츠에 적용이 어려운 단점이 있으며, 재생 시 처음 블록을 복호화 하는데 걸리는 재생 지연시간이 발생한다[4].

이 외에 국내외 DRM 솔루션들이 가지고 있는 문제점을 정리해보면 다음과 같은 문제점이 있다.

- 다양한 종류의 디지털콘텐츠의 포맷 지원 불가
- 수신자의 고유키 암호화로 인한 서버의 과부하
- 단일키 사용으로 보안 기밀성/무결성 보안취약
- 암호화 해제 시 콘텐츠의 기밀성 보안취약
- 대용량의 디지털 콘텐츠 암/복호화 소비시간

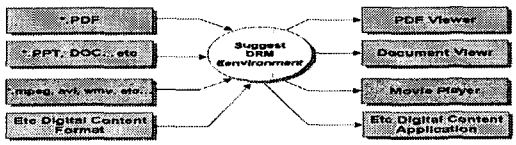
2.2 디지털 콘텐츠 헤더(Header)

디지털 콘텐츠를 분류해보면 문서파일, 그림파일, 음악파일, 동영상 파일, 실행파일, 라이브러리 파일, 시스템 파일, 압축파일 외에도 다양한 분류의 디지털 콘텐츠가 존재하며, 같은 분류의 콘텐츠라 할지라도 콘텐츠를 구성하는 포맷에 대한 정의에 따라서 많은 종류의 콘텐츠가 있다. 콘텐츠들의 내부 구조 포맷은 벤더들이 개별적으로 정의한 포맷이기 때문에 헤더 구성과 메인 데이터가 실리는 부분 및 기타 부가정보가 저장되는 부분들은 구조적 또는 위상적인 차이가 있을 수 있다[7].

디지털 콘텐츠에서 헤더는 실제 데이터(Main Data)의 선두에 놓여 있으며 콘텐츠에 대한 정보들의 모임으로써 일반적으로 데이터 내용, 데이터의 성격식별 정보, 데이터 제어정보, 버전정보, 파일의 길이, 파일의 다른 특성들을 기술하는 필드들로 구성되어 있고, 동영상 파일의 경우에는 콘텐츠가 사용한 압축 식별 정보(CompressionID)와 콘텐츠를 디코딩에 필요한 모듈식별정보(CodeID), 영상의 크기정보(Image Width/Height) 등의 필드로 구성되어 있다[7].

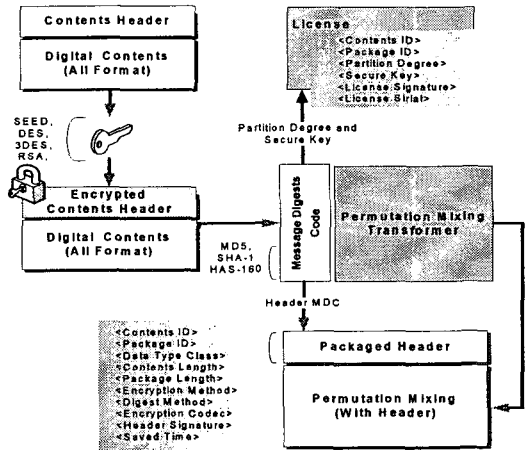
어플리케이션은 디지털 콘텐츠를 재생하기 전에 초기화 모듈에서 실제 데이터 부분을 재생할 수 있게 해주는 중요한 정보들의 집합인 헤더정보를 바탕으로 해서 실제 데이터를 읽어 들이기 위한 초기화 과정을 수행한다. 만약 메인 데이타 부분이 손상되었다면 에러체크 기법을 이용해서 에러에 대해 일부 복구가 가능하지만, 헤더가 손상될 경우에는 복구할 방법이 없으며 재생에 심각한 문제를 초래한다[7].

III. 제안하는 디지털 콘텐츠 보호기법



(그림 3) 제안하는 DRM 기법의 특징

본 논문에서 제안하는 콘텐츠 보호기법은 그림 3과 같이 모든 콘텐츠에 범용적인 DRM 보호기법을 적용하기 위해서 콘텐츠의 헤더정보를 검증된 암호 알고리즘으로 부분적인 암호화를 하고, 헤더를 포함한 콘텐츠 전체를 임의로 분할해서 콘텐츠 순열을 재조합 하는 기법으로서 콘텐츠 암호화 속도, 복호화 속도의 향상과 기존의 보안성을 유지하면서 유연하고 확장성 있게 디지털 콘텐츠를 보호하는 기법이다.



(그림 4) 제안하는 DRM 생성과정

그림 4는 제안하는 DRM 기법의 보호과정을 나타낸 것으로써 콘텐츠 헤더의 일정 크기 이상을 임의로 SEED, DES, 3DES, RSA 알고리즘을 하나 선택

하여 암호화를 수행한다. 단일 56비트 키를 사용하려면 DES를 선택하고, 높은 보안 및 오버헤드가 필요하지 않으면 3DES를 사용한다. 또는 강인한 보안을 필요로 한다면 AES 나 128비트 키를 사용하는 SEED를 선택하여 암호화를 수행 한다.

암호화된 콘텐츠의 위/변조 검사를 위해 무결성 알고리즘을 선택하여 MDC(Message Digest Code)값을 구한다. 이때 빠르게 사용한다면 128비트의 MD5를 선택하고, 보안성을 강하게 하려면 160비트 SHA-1 이나, HAS-160을 선택하여 수행 한다. 수행 속도를 빠르게 하려면 Level 1(DES / MD5), Level 2(3DES, MD5)를 사용하며, 보안을 강화하려면 Level 3(SEED, HAS-160), Level 4(RSA, SHA-1)의 조합으로 콘텐츠를 보호한다.

콘텐츠의 분할도에 따라서 암호화된 헤더를 포함한 전체 콘텐츠를 일정 크기로 순열조합변환기(Permutation Mixing Transformer)에 의해 순열 재조합이 이루 어 진다.

순열 재조합을 마친 DRM 보호된 콘텐츠에 대한 패키지 헤더가 설정되어 추가된다. 패키지 헤더는 제안하는 DRM 해석을 위한 최소의 정보가 다음과 같이 <Contents ID>, <Package ID>, <DataType Class>, <Contents Length>, <Packaged Length>, <Encryption Method>, <Digest Method>, <Encryptioin Codec>, <Header Signature> 등의 정보가 설정되어 그림 4에서 표현 한 것과 같이 DRM 콘텐츠의 헤더로 붙는다.

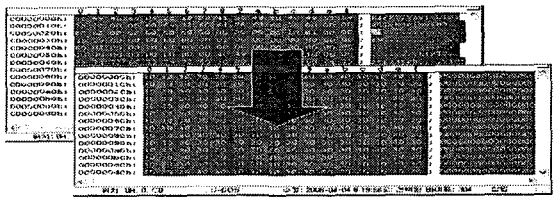
암호화에 사용된 비밀키와 콘텐츠 분할도는 사용자에게 보내질 라이선스에 <Contents ID>,<Package ID>,<Partition Degree>,<Secure Key> 등과 함께 하드웨어 디바이스 정보로 암호화되어 전송되어지게 된다. 따라서, 사용자측의 DRM 제어기(DRM Controller)에서만 라이센스를 획득하게 되고, 패키지된 헤더의 정보와 라이센스의 정보를 상호 평가하여 적절하게 콘텐츠가 정당한 절차에 의해 사용가능하게 되어 진다.

3.1 헤더 정보의 암호화

기존에는 디지털 콘텐츠 보호를 위한 암호화 방법으로 특정 포맷에 대하여 디지털 콘텐츠 포맷의 특정 필드의 정보를 암호화하는 맞춤식 보호방법 이었다. 이 경우에 *.mpeg을 보호하기 위한 DRM기법이라면 *.mpeg 포맷 특성에 제한적이기 때문에 다른 종류의 콘텐츠에 대해서 동일한 DRM 기법을 적용하기가 불가능하고, 콘텐츠의 포맷에 대한 분석이 이루어진 후에 연속되는 동일한 필드에 대해서 수백개 이상의 원하는 부분만 정확히 암/복호화가 수행되어야하므로 암호화와 복호화 속도 외에 부가적으로 콘텐츠 분석에 상당한 시간이 소요가 된다.

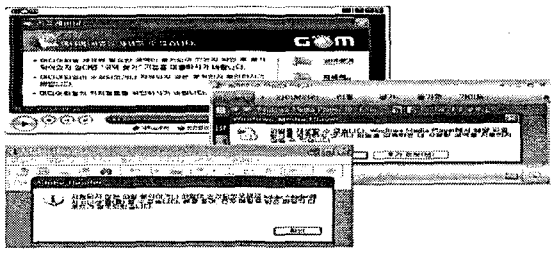
그러나, 디지털 콘텐츠 전체 중에서 선두에 위치한 극히 소량의 헤더정보 만을 SEED, DES, 3DES, AES 암호 알고리즘 중에서 선택하여 암호화시키고 암호화 시킨 부분에 대한 해쉬값 (MDC:Message Digest CheckSum)을 저장하여 헤더의 무결성을 평가한다. 따라서 부분 헤더 암호화를 수행하게 되면 콘텐츠 전체에 대해 영향을 끼칠 수 있으면서도 기존의 암호화와 복호화 속도에 비해서도 상당히 빠른 결과가 나오게 되며, 콘텐츠 전체에 대한 보안을 유지할 수 있다.

미디어 파일일 경우 헤더부분이 정상적이고 실제 데이터에 손상이 되었을 경우는 인덱스를 재구성하는 프로그램들로 복구가 가능하지만 현재 완벽한 프로그램은 없으며, 반대로 헤더부분이 손상된 경우에도 복구하는 3rd Party 프로그램이 존재 한다고는 하지만 헤더는 복구가 불가능한 걸로 알려져 있다.



(그림 5) WMV9 콘텐츠 헤더부분 암호화

그림5와 같이 WMV9 미디어 파일포멧의 Header Object는 선택적 Object와 필수 Object가 있는데, Header Object에 포함되는 정보는 콘텐츠가 사용한 압축식별정보(CompressionID)와 콘텐츠를 디코딩에 필요한 모듈식별정보(CodecID), 영상의 크기 정보(ImageWidth / Height), 및 콘텐츠 실행에 필수적인 정보들이 기술되어 있는 것을 확인할 수 있다.



(그림 6) 암호화된 콘텐츠의 재생 실험 화면

디지털 콘텐츠 헤더부분에서 선두 데이터 일부분을 암호화해서 이후 실제 데이터(Main Data) 부분까지 영향을 끼치게 되고 그림 6 테스트에서와 같이 해당 어플리케이션에서 재생 할 경우 재생할 수 없다고 메시지를 출력한다. 또한, 다른 종류의 디지털 콘텐츠 포맷인 아크로뱃의 *.pdf 문서에 대해서도 동일한 방식으로 헤더부분을 암호화 함으로 해서 재생할 수 없다는 메시지를 출력하는 것을 확인할 수가 있다.

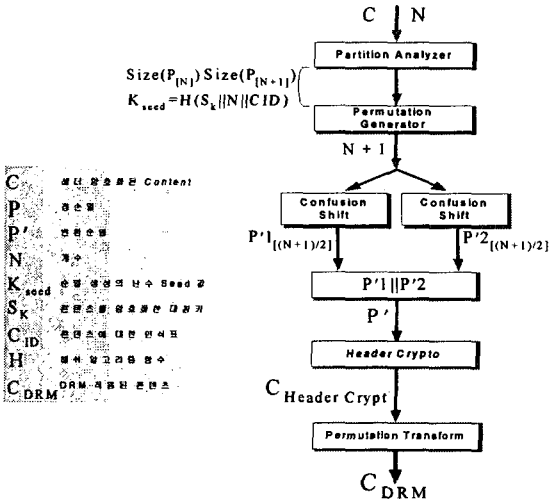
이와 같이 헤더부분만을 부분 암호화 하는 방법으로 모든 콘텐츠에 동일하게 헤더 일정 부분을 암호화 특정 콘텐츠에 제한되지 않고, 유연하고 확장성 있게 모든 종류의 디지털 콘텐츠에 적용가능 하다.

3.2 콘텐츠 분할 순열조합 방법

순열 재조합 방식은 3.1절에서 제시한 방법과 병행하여 사용하는 방법으로 헤더의 암호화만으로는 실제 데이터 부분의 보안성이 부족하다고 판단된다. 따라서, 표1에서 도출한 요구사항을 만족하면서 콘텐츠 전체에 대한 보안성을 향상 시키는 방법을 제안한다.

디지털 콘텐츠들을 임의로 N+1 개로 분할할 경우에 정확한 조각 크기와 순서가 맞아야만 정상적인

재생을 할 수가 있게 된다. 그러나, 분할된 조각에 대한 순열이 특정한 규칙에 의해 섞일 경우 정상적인 순열로 정확히 일치시키지 못하고, 조각의 크기들을 맞추지 않으면 해당 콘텐츠에 대한 접근이 불가능하게 된다.



(그림 7) 헤더 암호화와 순열조합 구조

분할 초기의 순열로 이루어진 완전한 콘텐츠를 N+1 개로 분할하기 위해 분할 분석모듈은 전체 크기와 분할될 부분들의 크기를 분석하고, 순열 생성기에서는 $K_{seed}=H(S_k||N||CID)$ 를 난수생성 Seed 값으로 확률분포가 일정한 RNG 모듈을 통해 난수 순열 표를 생성한다. 생성된 순열 표의 순서 배열에 대한 복잡도를 고려하여 확산 이동 모듈에서는 N/2개로 나눈 후 순열 이동을 시켜서 예측하기 어렵도록 복잡한 하나의 순열 표를 생성하게 된다.

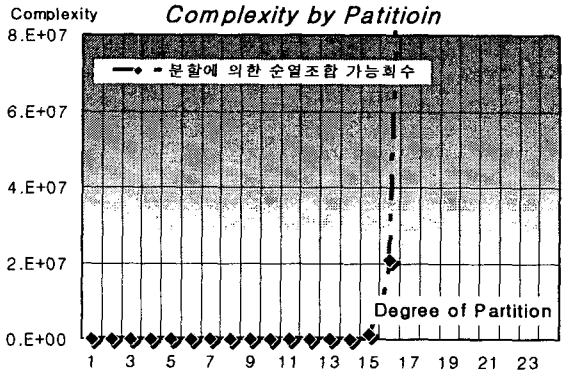
IN Permutation	1	2	3	4	5	6	7	8	9	10
OUT Permutation	5	10	2	6	4	9	1	7	3	8

(표 2) K_{seed} 값으로 생성된 순열 표

그리고, K_{seed} 키를 생성하기 위해 사용되었던 비밀키(S_K)로 콘텐츠에 대한 헤더부분을 암호화한 후에 순열 변환모듈은 표3과 같이 생성된 순열 표를 참조하여 실제 분할된 콘텐츠를 재조합을 수행하게 된다. 따라서, 암호화된 헤더 부분과 전체 부분을 추측하기 힘들도록 재조합된 DRM 보호기법이 적용된 콘텐츠가 생성된다.

분할도가 15로 분할되었을 경우 추측 가능한 수는 870억개 이상의 조합이 필요하고 16일 경우는 1조 3,000억, 20일 경우에는 1,216천조의 조합이 발생한다. 이는 그림 9에서 보는 바와 같이 15분할 이후 부터는 조합가능 회수가 기하급수적으로 증가함을 알 수가 있고, 분할도가 높을수록 추측에 의한 순열 재조합은 불가능 하게 된다고 할 수 있다.

또한, 콘텐츠의 재생을 위해서는 우선 콘텐츠 헤더의 일정 부분 암호화에 대한 비밀키 값을 알아야 하고, 분할도를 알아야 하며, 분할에 따른 순열을 알아야만 정상적으로 콘텐츠에 접근이 가능 하다. 이러한 값들 중 하나라도 잘못된 정보가 들어간다면 콘텐츠는 재생이 불가능 하게 된다.



(그림 8) 예측 가능한 재조합 시도회수

IV. 결론

기존의 DRM 기법은 특정 콘텐츠 포맷에 제한적이고 정적인 보호방법으로 다양한 콘텐츠에 적용할 수 없다. 그리고 콘텐츠 전체에 대한 분석과 많은 양의 데이터에 대한 암호화가 수행되므로 속도가 느린 단점이 있으며, 단일 키를 사용해서 키의 노출에 의한 보안위험도 있을 수 있다.

본 논문에서 제안하는 DRM 보호기법은 디지털 콘텐츠의 포맷에 제한없이 모든 콘텐츠에 적용 및 보호 가능하고, 암호화 속도의 향상을 위해 디지털 콘텐츠를 재생하는데 필수정보인 헤더부분만을 암호화 하여 암/복호화 수행 속도를 향상시켰으며, 분할된 콘텐츠의 순열을 재조합하는 방법을 설계 하였다. DRM 보호기법의 보안성과 확장성 및 범용적 사용을 지원할 수 있을 것이며, 새로운 환경과 콘텐츠에 대해서 능동적으로 보호가 가능하여 다양한 응용분야에 활용 가능할 것 이다.

[참고문헌]

[1] 박정선, 공공부분 IT 신기술 응용과제 발굴 및 적용 방안에 관한 연구, 한국전산원, 2004.
[2] 강호갑, DRM 최신 국제표준 기술사양 분석 및 세계 유명제품 동향과 전망에 관한 연구, 한국정보처리학회, 2004.
[3] 김현곤, DRM 활성화를 위한 공공사업안 발굴(안), 한국전산원, 2005.
[4] 김정재, 이경석, 전문석, 시큐리티 에이전트를 이용한 사용자 인증과 DRM 보안시스템 설계, 정보처리학회논문지C, 제12-C권 제7호, 2005.12.
[5] 전종미, 최영철, 박상준, 박성준, DRM 기술 및 제품 동향 분석, 정보보호학회논문지 제11권 제5호, 2001.10.
[6] 김후종, 나승원, 무선 인터넷 환경에서 디지털 콘텐츠 저작권 보호를 위한 모바일 보안 시스템의 설계 및 구현, 정보처리학회논문지 제10-C권 제6호, 2003.10.
[7] 정병옥, 장재혁, 최용락, 분할된 콘텐츠의 순열조합을 이용한 범용 DRM 보호기법 설계, 한국인터넷정보학회 춘계학술발표, 2006.4.