DRM 시스템에서 해쉬체인과 세션키 교환을 이용한 암호화 기법에 관한 연구

박 찬 길[†] · 김 정 재[††] · 이 경 석[†††] · 전 문 석[††††]

요 약

본 논문에서는 기존의 암호화 방법보다 안전한 키를 생성하는 해쉬체인 알고리즘을 제안하며, 해쉬체인 알고리즘 기법을 통해 생성한 각각의 키를 각각의 블록에 적용한 암호화 방법을 사용하여 기존의 시스템보다 보안성이 높은 암호화 방법을 제안한다. 또한 사용자 인증기법을 통해 사용자를 유/무선으로 인증한 후, 키 분할 기법을 이용하여 분할된 키를 안전하게 전송하는 방법과 클라이언트에 키가 유출 되어도 완전한 키를 얻지 못하도록 하는 세션키 분할 기법을 제안한다. 제안한 시스템을 설계하고 구현한 후 성능 평가를 위해 다양한 크기의 디지털콘텐츠 파일을 이용하여 실험을 수행하였으며, 제안한 시스템이 기존 시스템에 비해 안전한 키 전송을 할 수 있었고, 키 유출에도 전체 데이터를 복호화 할 수 없도록 암호화 하였다. 또한 클라이언트 시스템에서 비디오 데이터 파일 재생 시 암호화·복호화 시간은 기존 방법과 유사함을 확인하였다.

키워드 : 저작권보호, 대칭키, 세션 인증, 세션키 교환

A Study on Encryption Method using Hash Chain and Session Key Exchange in DRM System

Chan-kil Park[†] · Jung-jae Kim[††] · Kyung-seok Lee[†††] · Moon-seog Jun[††††]

ABSTRACT

This is devoted to first, to propose a hash chain algorithm that generates more secure key than conventional encryption method. Secondly, we proposes encryption method that is more secure than conventional system using a encryption method that encrypts each block with each key generated by a hash chain algorithm. Thirdly, After identifying the user via wired and wireless network using a user authentication method. We propose a divided session key method so that Although a client key is disclosed, Attackers cannot catch a complete key and method to safely transfer the key using a divided key method. We make an experiment using various size of digital contents files for performance analysis after performing the design and implementation of system. Proposed system can distribute key securely than conventional system, and encrypt data to prevent attacker from decrypting complete data although key may be disclosed. The encryption and decryption time that client system takes to replay video data file is analogous to the conventional method.

Key Words : DRM, Symmetric Key, Session Authentication, Session Key Exchange

1. 서 론

인터넷 사용의 보편화로 인해 사이버 공간을 통한 디지털 정보의 변화가 가속되고 있으며, 이러한 디지털 정보의 자원에 대한 유통 환경이 급속히 변화함에 따라 디지털 형태의 음악, 화상, 영상물, 출판물 등 디지털콘텐츠에 대한 수요가 급격히 증가하고 있다. 하지만 디지털 콘텐츠로의 전환이 가져오는 맹점으로는 디지털 저작물의 품질에 대한 손상이 없이 복제가 가능하기 때문에 불법복제 방지를 위한 디지털 저작권 보호문제가 중요한 이슈로 대두되고 있다. 디지털 저작물 보호를 위해서는 안정성과 보안성 확보를 위하여 정보보호 기술이 필요하고, 디지털 저작권과 저작물 유통의 전반을 감시하고 추적하기 위한 디지털 저작권 관리(DRM : Digital Rights Management) 기술이 필요하다[3]. DRM 기술을 통해 디지털 저작물에 대한 지적재산권 침해 사례로부터 저작권을 보호하고, 유통과정을 관리하기 위한 종합적인 대책이 추진되어 저작물 제작, 유통, 이용 등이 일련의 신뢰할 수 있는 환경에서 이루어질 수 있도록 하는 다양한 연구가 진행 중에 있다[5]. 기존 DRM 솔루션들은 암호화에 사용하는 키로 비밀키를 사용하여 사용자가 파일을

† 정 회 원 : 한성디지털대학교 멀티미디어학과 교수
†† 정 회 원 : (주)RetailTech 수석연구원
††† 종신회원 : 건국대학교 정보통신대학원 겸임교수, 산업연구원 연구위원
†††† 종신회원 : 숭실대학교 교수
논문접수 : 2006년 5월 4일, 심사완료 : 2006년 8월 9일

다운로드할 때 암호화를 수행하므로 많은 시간이 소요가 된다. 또한 복호화를 수행하는 경우에도 대용량의 저작물인 경우 전체 파일에 대하여 복호화를 먼저 수행한 후에 실행을 할 수 있으므로 사용자가 실시간으로 파일을 플레이해서 볼 수 없는 문제점이 있으며, 암화화 및 복호화에 사용되는 비밀키가 유선상으로만 암호화되어 전송이 되기 때문에 다른 악의적인 사용자에 의하여 노출이 된다면 해당 저작물에 대한 보호는 더 이상 보장하지 못하는 단점이 있다[2].

따라서 본 논문에서는 기존의 DRM 시스템이 가지는 문제를 해결하기 위해 유·무선을 통한 키 전송 방법을 사용한 DRM 시스템을 제안하여 디지털 저작물에 대한 사용자 인증과 암호화 된 데이터 자체의 복호화 키를 분배하고, 불법적인 실행을 방지할 수 있는 통합적인 DRM 시스템을 제안한다.

2. 관련 연구

2.1 DRM 연구 현황

디지털 저작물은 품질의 손상 없이 복제가 가능하기 때문에 불법복제로부터 저작자를 보호하기 위해 안전한 디지털 저작권 보호시스템의 개발이 필요하며, 이를 보완하기 위하여 허가되지 않은 사용자로부터 디지털 저작물을 안전하게 보호함으로써 저작권자의 권리 및 이익을 지속적으로 보호하는 다양한 연구가 진행 중에 있다. 특히 유선 인터넷망에 적용되어온 DRM 기술이 무선인터넷 망의 발달로 인해 무선 콘텐츠 시장으로 확대 되고 있다.

2.2 InterTrust의 DRM 시스템

InterTrust사의 DRM 솔루션 특징은 저작물의 보호를 위해서 암호기술과 워터마킹을 사용하며 저작물 사용규칙을 지정하여 사용내역의 수집 및 기록, 과금 처리를 수행하는 것이다. 사용자 컴퓨터에 에이전트를 실행하여 라이선스와 과금 처리, 저작물의 실행을 에이전트를 통하여 처리하도록 하였다. 저작물은 사전에 암호화되어 배포되므로 사용자의 컴퓨터에서 저작물을 사용하는 시점에서 라이선스 에이전트가 라이선스를 확인하고 지불정보를 전송하여 거래를 체결하도록 하였다. 그러므로 신용카드나 전자 화폐 등의 결제 방식을 이용하여 거래할 수 있다[8-10]. 또한 저작물이 암호화되어 보호되고 있으므로 사용자들 사이에 암호화된 저작물을 주고받을 수 있는 저작물 재분배(SuperDistri- bution)를 실현하였다[4].

하지만 InterTrust사의 DRM 시스템의 복호화는 (그림 1)과 같이 복호화가 끝난 후에 재생이 가능하다.
또한 1개의 키로만 암호화 하기 때문에 키가 유출이 될 경우 더 이상 보호를 받지 못한다는 점과 파일 전체를 암호화하기 때문에 암호화/복호화 하는데 시간이 다른 시스템보다 오래 걸리는 점과 재생시 전체 복호화가 끝난 후에야 재생이 되는 단점이 있다.

(그림 1) InterTrust사의 DRM 시스템

2.3 Microsoft의 DRM 시스템

Microsoft의 DRM 시스템은 저작물 제공자와 소비자들에게 디지털 미디어 파일을 안전하게 분배하는 종단 간(end-to-end) DRM 시스템이다[11]. 핵심 제어 부분은 WMRM(Windows Media Rights Manager)으로서 저작물 제공자에게 인터넷 상에서 암호화된 파일 형식으로 보호된 음악, 비디오 등의 미디어를 개인의 컴퓨터, 휴대용 재생 장치, IP 네트워크에 연결된 네트워크 장치에 배달한다[11]. WMRM에서 각각의 서버 또는 클라이언트 인스턴스들은 개인화(indivisualization)과정을 통해 키 쌍을 할당받게 되며, 크래킹 되었거나 안전하지 않다고 판단되는 인스턴스에 대해서는 인증서 취소목록을 이용하여 서비스 대상에서 제외시키게 된다. 인증서 취소목록은 마이크로소프트사의 웹사이트를 통해 배포된다. 키는 라이선스에 포함되고, 라이선스와 저작물은 분리되어 분배되기 때문에 저작물 재분배를 지원한다.

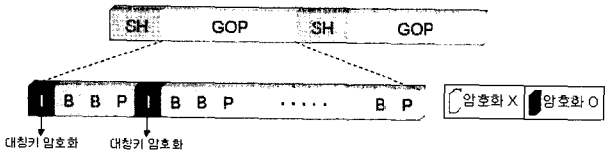
하지만 Microsoft사의 DRM 시스템의 경우는 자사의 WMV와 WMA의 파일 포맷만을 지원하기 때문에 암호화시 파일 전체를 인코딩하여 암호화하기 때문에 시간이 오래 걸린다.

2.4 I-Frame DRM 시스템

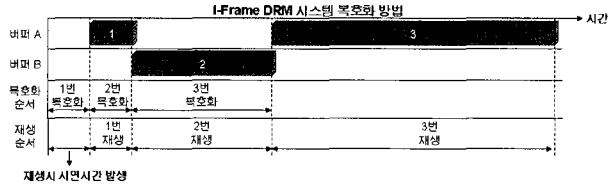
I-Frame DRM 시스템은 (그림 2)와 같이 동영상 GOP (Group Of Picture)의 I-Frame을 대칭키를 이용하여 AES 알고리즘이나 SEED 알고리즘 중에서 하나를 선택하여 암호화한 후 해당 콘텐츠의 ID(CID)와 대칭키의 값을 서버의 데이터베이스에 저장한다[2].

사용자가 암호화된 동영상을 실행시키면 사용자의 인증서를 이용하여 사용자 인증을 수행한 후 서버는 암호화에 사용된 키 값을 사용자의 공개키로 암호화 시키고, 사용자는 개인키를 사용하여 암호화에 사용된 대칭키 값을 획득한 다음, 동영상의 I-Frame만을 다시 복호화 시켜 B, P 프레임과 함께 버퍼에 저장하여 플레이 한다.

I-Frame DRM 시스템은 (그림 3)과 같이 전체 동영상의 복호화가 끝나기 전에 해당 파일을 재생할 수 있는 이중 버퍼 알고리즘을 사용한다. 이 I-Frame DRM 시스템은 MPEG(Moving Picture Expert Group)데이터에서 I-Frame



(그림 2) I-Frame DRM 시스템의 암호화 방법



(그림 3) I-Frame DRM 시스템의 이중 버퍼를 사용한 복호화 방법

만을 암호화하기 때문에 부분 암호화 시스템에 속하며 이는 암호화 및 복호화 속도가 기존의 다른 시스템보다 향상된 시스템이며 일부분만 복호화 한 후 재생하는 방법으로 실시간적인 서비스를 많이 제공해 주는 시스템이다.

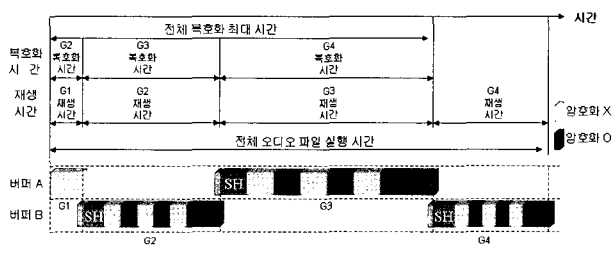
하지만 I-Frame을 추출하기 위하여 GOP(Group of Picture) 그룹의 모든 헤더의 내용을 읽은 다음 I-Frame의 크기를 계산하여 복호화 하는 시스템이다. 동영상에서 I-Frame의 개수가 1시간의 영화일 경우 약 86,000개이기 때문에 이를 계산하는데 시간이 많이 소요가 되며, 한 개의 키 만을 사용하기 때문에 키가 유출이 되면 더 이상 암호화된 동영상은 보호를 받지 못한다는 단점과, 재생 시 처음 블록을 복호화 하는데 걸리는 재생 지연시간이 발생한다.

2.5 부분 암호화 시스템

부분 암호화 시스템은 기존의 암호화 시스템에서 사용한 하나의 키로만 암호화하는 방법 대신 디지털 콘텐츠를 n개의 블록으로 나눈 후에 키 생성 알고리즘을 통해 생성된 서로 다른 키로 m개의 블록만을 암호화 시키는 시스템이다. 이는 하나의 키가 유출이 되었을 때 더 이상 콘텐츠 보호를 하지 못하는 단점을 해결하기 위해 사용된 방법이다[1].

부분 암호화 시스템에서 생성된 m개의 키는 서버에 직접 저장을 하지 않고, 클라이언트에서 복호화 시 각각의 키를 유추하여 재생시킬 수 있다. 또한 콘텐츠 재생 시 실시간성을 보장하고, 콘텐츠의 모든 블록이 암호화 되어 있지 않기 때문에 연산능력이 낮은 장치 및 하나의 키가 유출이 되더라도 동영상 전체가 복호화 되지 않는 특징을 가지고 있다.

하지만 (그림 4)에서 처럼 모든 블록이 암호화 되지 않았을 경우, 콘텐츠의 중요한 블록이 암호화 되지 않을 수도 있으며, 키 복호화시 중요한 요소인 CID(콘텐츠 ID)값을 SSL 채널을 통한 세션 ID 값과 단순히 XOR를 사용하여 세션 ID값을 얻기 때문에 보안성이 취약하다는 단점이 있다.



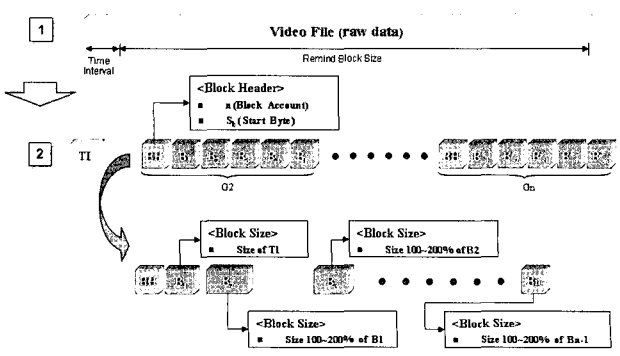
(그림 4) 부분 암호화 DRM 시스템

3. 제안 시스템 구조

3.1 암호화 과정

(그림 5)와 같이 디지털콘텐츠를 암호화하기 전에 원시데이터(Raw Data)를 블록으로 나누어 각각의 블록을 암호화할 수 있도록 전 처리작업을 수행한다. 전 처리작업 수행시 첫 번째 암호화 블록은 원 데이터가 시작되기 전에 지연시간(TI : Time Interval) 만큼을 첫 번째 블록크기로 정하고 두 번째 블록의 크기는 전 블록크기의 100~200% 내에서 블록으로 나누어 처리한다. 블록크기를 전 블록크기의 100~200%로 설정함으로 데이터가 무한 수렴하는 것을 방지할 수 있었으며, 원시 데이터의 크기에 따라 적절한 양의 블록을 생성할 수 있어 복호화 처리 시 실행속도가 가장 안정적으로 나타났다. 그룹생성 시 몇 개의 블록을 묶어 하나의 그룹으로 나타내고, 하나의 그룹은 첫 번째 블록의 12배 내에서 하나의 그룹으로 묶어 처리하였다. 첫 블록의 12~13배 사이에서 복호화 후 실행 시 이중 버퍼를 상용하여 실행하였을 때 처리지연시간이 발생하지 않았다. 두 번째 그룹에서 마지막 그룹까지 같은 방법으로 그룹화 하며 블록을 몇 개의 그룹으로 그룹화 하는 것은 암호화 또는 복호화시 보상이중버퍼를 이용하여 암·복호화시 처리속도를 향상시켜 안정된 암호화 기법을 제공할 수 있기 위해서이다.

디지털콘텐츠를 입력받아 파일사이즈를 확인하고 배열을 초기화하여 블록단위로 처리할 수 있도록 준비한다. 영상을 처리하기 전에 지연시간을 체크하여 지연된 시간의 크기를 저장한 후 첫 번째 블록의 크기를 지연시간의 크기로 나누어 암호화 시 같은 크기로 적용한다. 첫 번째 블록을 암호화 한 후 데이터가 남아있는지 확인한 후 남은 데이터가 없으면 블록단위로 나누는 것을 종료한다. 남아있는 데이터가 있으면 앞 블록크기의 100~200% 사이의 크기로 랜덤함수를 적용하여 나누어 블록으로 나눈다. 계속하여 반복하여 남아있는 데이터 없을 때까지 블록으로 나눈다. 이중버퍼를 사용하여 복호화 할 때 끊임없이 처리할 수 있는 그룹의 크기는 지연시간 크기의 12배까지 묶어서 하나의 그룹으로 묶어주고, 나머지 블록들을 다시 전 블록의 마지막 블록크기의 12배까지 묶어 두 번째 그룹으로 묶어준다. 계속하여 남은 블록이 없을 때 까지 반복하여 그룹으로 묶어줌으로써



(그림 5) 디지털 콘텐츠 블록 분할 기법

〈표 1〉 복호화 시간과 플레이 시간 비교

Interval	Decryption time		Playing time	
	Time (second)	Size (Kbyte)	Time (second)	Image size (Kbyte)
G1	0.1	508	0.1	40
G2	1.238	6287	1.238	508
G3	15.328	77,841	15.328	6,287
G4	189.785	963,752	189.785	77,841
G5	2349.720	11,932,174	2349.720	963,752

복호화 시 그룹단위로 상호이중 버퍼를 적용하여 복호화 함으로써 복호화 시 걸리는 지연시간을 줄여 데이터 실행시 중단되는 현상을 막을 수 있도록 하였다. <표 1>과 같이 복호 화시 이중버퍼를 사용하여 실행과 복호화를 동시 시행함으로써 끈임이 없이 처리 할 수 있다.

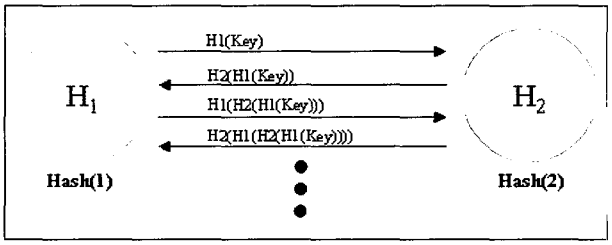
전처리 작업으로 초기 파일사이즈를 체크 할 수 있도록 하였으며, 배열을 두어 블록단위로 처리 할 때 블록의 크기 값을 보관하도록 설계하였다. 콘텐츠 실행시 시간지연시간을 체크할 수 있도록 하였으며, 디지털 콘텐츠의 남은 크기를 계산하여 다음 블록의 크기로 분할 할 수 있도록 하였다. 분할된 블록을 이용하여 그룹화 하였으며, 블록이 없을 때까지 반복하여 그룹으로 묶어 처리한다.

3.2 Hash Chain기법을 이용한 암호화 Key 생성 설계

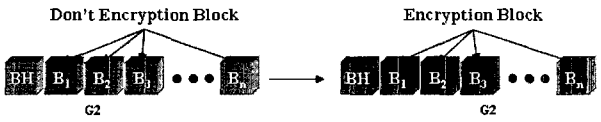
분할된 블록을 암호화 하기위하여 서로 다른 두개의 해쉬 함수(Hash Function)를 사용하여 사용자 인증번호로 첫 번째 해쉬 함수(H1)에서 키를 생성하고, 생성된 키를 이용하여 첫 번째 블록을 암호화한다.

(그림 6)은 첫 번째 생성된 키값을 해쉬하여 두 번째 해쉬 함수(H2)에서 다시 키를 생성하고, 생성된 키를 이용하여 두 번째 블록을 암호화 한다. 두 번째 해쉬함수(H2)에서 생성한 키를 다시 H1 함수로 보내어 세 번째 키를 생성하고 생성된 키를 이용하여 세 번째 블록을 암호화한다.

이러한 방법으로 남은 콘텐츠가 없을 때까지 계속 반복하여 모든 블록이 암호화 될 때까지 반복하여 키를 생성할 수 있도록 이중 해쉬 함수를 이용하여 키를 생성하고 암호화를 진행한다. 두개의 해쉬 함수를 이용하여 디지털콘텐츠를 암호화함으로써 암호화의 안전성을 높일 수 있으며 하나의 키가 유출되어도 해쉬 함수 알고리즘을 알 수 없으므로 다른 블록들을 복호화 할 수 없도록 한다.



(그림 6) 해쉬체인 방법을 이용한 키 생성방법



(그림 7) 디지털콘텐츠 블록분할 처리

제안 논문에서는 (그림 7)과 같이 분할 알고리즘을 이용해 분할 된 데이터 들을 이중 해쉬 알고리즘을 이용하여 키를 생성하고 생성된 키를 이용하여 각각의 블록을 암호화 한다. 암호화시 그룹 내의 블록의 위치주소 및 크기정보를 가지는 Block Header(BH)와 전체그룹을 제어하는 정보는 LAU (License Acquisition URL)와 Contents ID로 이루어진 Container Header(CH)로 구성되어 있으며, Main Header (MH)는 그룹의 크기와 DID를 해쉬한 값을 가지고 있다.

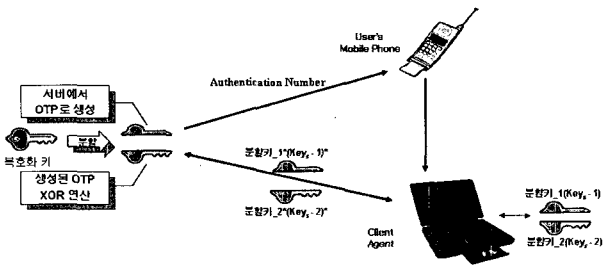
암호화된 각각의 블록에 대한 정보를 블록헤더(BH)에 두어 그룹 내의 블록의 개수와 각 블록의 시작 비트의 정보를 가지고 있도록 하였다. 또한 전체 데이터를 관리할 수 있도록 하기 위하여 컨테이너헤더(CH)를 두어 콘텐츠 ID와 각각의 블록 헤더의 시작위치 정보를 저장하도록 하여 복호화 시 처리 속도를 높일 수 있도록 하였다.

서버에 메인헤더(MH : Main Header)를 두어 콘텐츠의 각각의 그룹 사이즈와 장치 ID를 저장하여 인가된 사용자에게 제공할 수 있도록 하였으며, 콘텐츠의 유출시 인가된 사용자에게 메인 헤더 정보를 제공함으로써 콘텐츠 유출에도 안전성을 확보 할 수 있도록 하였다.

3.3 사용자 인증 및 키 전송 기법 설계

시스템의 전체적인 개요는 정보유출 방지 및 사용자 확인을 위하여 서버는 인증된 사용자를 확인한 후 무선으로 사용자 인증번호(UAN : User Authentication Number)를 제공한다. 사용자는 인증번호를 키 값으로 입력하여 복호화 키를 유선으로 요청하게 한다. 사용자 인증번호를 확인한 에이전트는 OTP(One Time Password)로 복호화 키를 생성하여 생성된 키를 안전한 방법으로 사용자에게 제공하는 알고리즘을 통해 키를 제공한다.

생성된 키는 키 분할 알고리즘을 이용하여 두개의 키 (Keys_1, Keys_2)로 분할 한 후 에이전트를 이용하여 Keys_1과 Keys_2를 각각 암호화 하여 사용자에게 전송하는 절차를 거쳐 키 값을 (그림 8)과 같이 전송한다.



(그림 8) 복호화 키 생성 및 전송 기법

키 분할 알고리즘은 다음과 같다.

키 분할 알고리즘 : $Key \oplus OTP = Temp$ (식1)
$OTP(Ka)$: $Keys\_1$ $Temp(Kb)$: $Keys\_2$

안전한 키 전송을 위하여 사용자 인증과정을 통해 사용자를 확인한 후 사용자에게 전송할 키를 OTP를 이용하여 키를 생성한 후 생성된 키를 전송하는 키 전송 프로토콜을 다음과 같이 제안하였다(그림 9)

Ka를 Keys_1이라하고, Kb를 Keys_2라 하여 두 번에 나누어 제공 할 수 있도록 하였다.

첫째 UAN(ex : 101023)는 서버에서 생성하여 사용자에게 SSL 채널을 통해 모바일로 제공함으로써 사용자에게 안전하게 제공할 수 있도록 하였다.

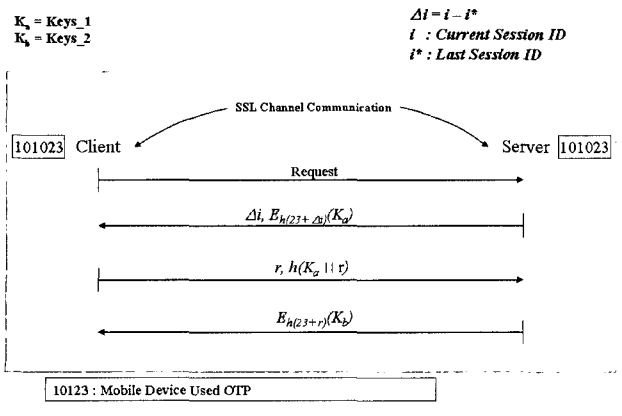
둘째 UAN을 이용하여 복호화 키를 요구할 수 있도록 하였으며, 처음 사용자는 인증번호를 이용하여 복호화 키를 요청하면 서버는 키 분할 알고리즘(식1)을 이용하여 키를 생성한 후, 키 전송 프로토콜을 이용하여 안전하게 키를 제공받는다.

셋째 서버는 세션 증가값(Δi)과 UAN을 더한 값을 암호화 키로 사용한 암호화된 Ka값을 클라이언트로 전송을 한다.

넷째 사용자는 Ka를 복호화 한 후, 난수 값 r을 생성하여 Ka값과 r 값을 연접(Concatenation)하여 해쉬한 후, 서버로 다시 전송을 하게 된다.

마지막으로 서버에서는 클라이언트에서 발생한 난수값 r값과 UAN을 더한 값으로 다시 암호화 하여 Kb를 전송한다.

처음 사용자와 재 사용자를 구별하여 재사용자는 이중으로 키를 요구하지 않고도 계속 사용할 수 있도록 이전 사용하던 세션 값 i를 보관하고 있다가 서버에 세션 값을 확인한 후 계속 사용할 수 있도록 설계하였다. i는 세션 값을 나타내며 Δi는 세션의 증가 값으로 이전 세션을 i*이라하고 i를 현재 세션 값으로 정의하여 계속 사용자에게는 세션 증가 값을 확인하여 계속 사용할 수 있도록 하고, 처음 사용자는 세션의 증가 값이 없으므로 키 값을 제공받아 사용하도록 하였다.



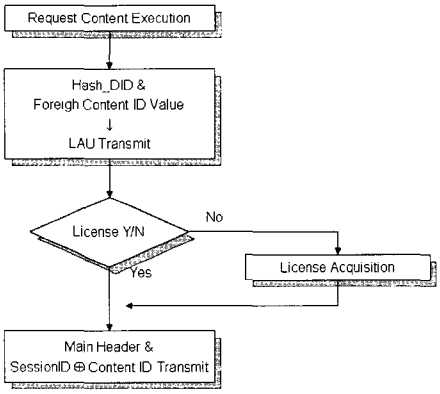
(그림 9) 키 전송 프로토콜

3.4 복호화 과정

디지털콘텐츠 복호화 과정은 Container의 Content ID와 동일한 라이선스 유/무 확인한다. 라이선스가 없을 때는 Container Header의 LAU(License Acquisition URL)로 이동하여 라이선스 취득하고 사용자의 DID(Device ID : Mac Address)를 해쉬값으로 저장한다.

(그림 10)과 같이 동영상을 실행요청을 하려고 할 때 처음 사용자는 라이선스를 할당 받아 라이선스를 이용하여 복호화를 할 수 있도록 한다. 키 획득시에는 사용자 인증과정과 복호화에 필요한 복호화 키를 수신한다. Content ID로 해당 디지털콘텐츠 MH(Main Header)를 요청하고 MH에 사용자의 해쉬한 DID값과 Main Header를 사용자 공개키로 전송한다. 개인키로 메인 헤더 복호화 후 자신의 컴퓨터와 메인 헤더에 포함된 해쉬 값과 같은지 확인 후 재생한다.

MH(Main Header)는 사용자의 공개키 PU를 사용하여 암호화(Epu(MH)하여 사용자의 개인키로 MH를 복호화한다. BH의 위치 획득 후 사용자 인증 기법을 통해 Key 획득하며 BH의 내용을 Key로 Gk(B1~Bn)의 내용을 복호화한다.



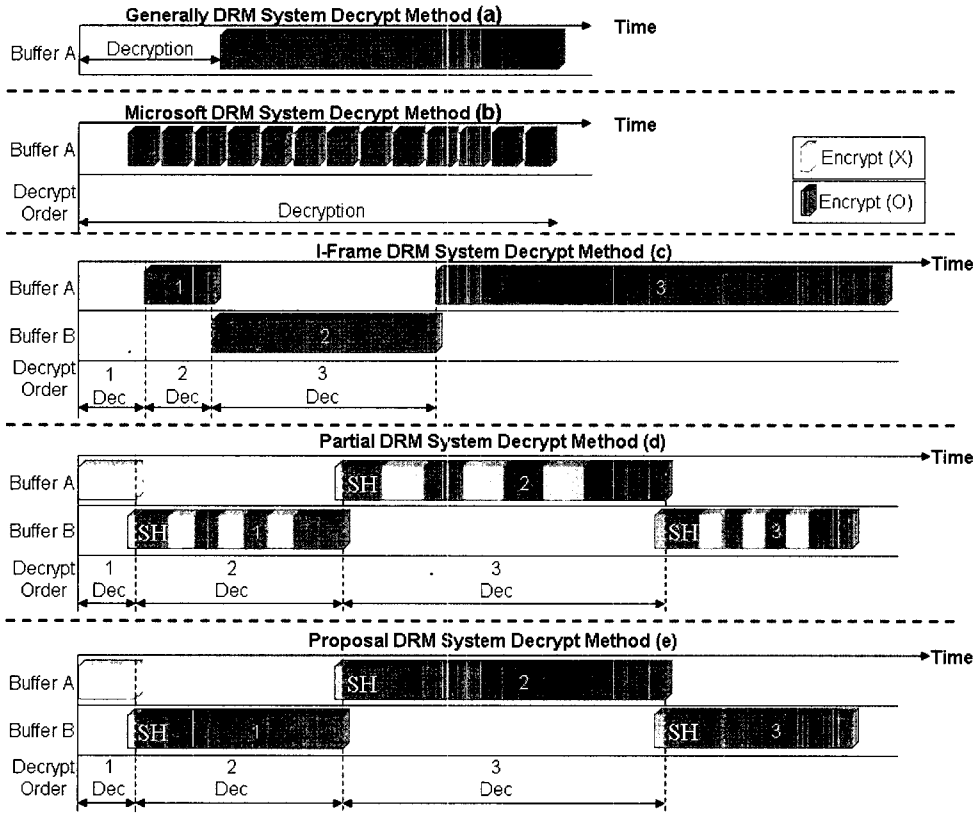
(그림 10) 복호화 시 라이선스 인증 기법

4. 실험 평가

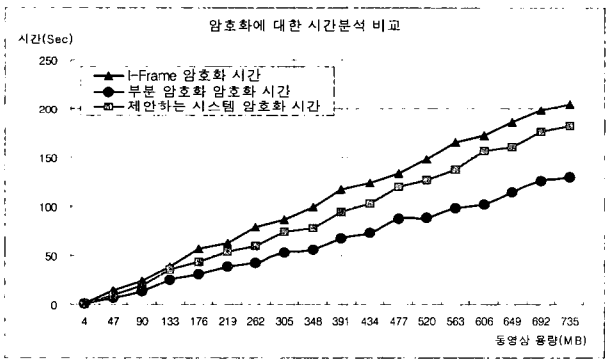
4.1 지연시간에 대한 평가

암호화된 디지털 콘텐츠 재생시 복호화 시간을 분석하여 재생시간을 비교하였다. 기존 복호화 알고리즘과의 지연시간에 대한 비교를 통해 제안된 알고리즘의 지연시간을 (그림 11)에서 비교분석하였다.

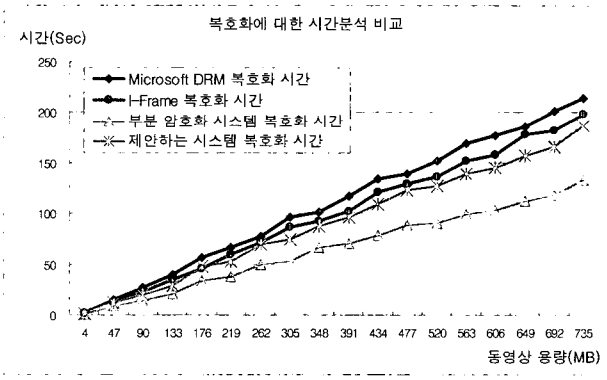
기존의 마이크로소프트의 DRM시스템(b)은 전체 암호화된 자료를 일정크기의 버퍼에 복호화 한 후 재생하므로 초기 재생시 지연시간이 발생을 하며, 버퍼 언더플로우 발생시에도 지연시간이 발생하는 문제점이 있다. 동영상을 구성하고 있는 I, B ,P 프레임에서 I 프래임만을 뽑아서 암호화 하는 방법인 I-Frame 시스템의 복호화(c)는 일부분을 복호화한 후 이중버퍼를 사용하여 처리지연시간이 적게 발생하였다. 부분 암호화 시스템(d)는 I-Frame 시스템과 같은 이중 버퍼 알고리즘을 사용하였으며, 지연시간이 전혀 발생하지 않는



(그림 11) 기존 시스템과의 지연 시간에 대한 분석



(그림 12) 암호화에 대한 시간 분석 비교 그래프



(그림 13) 복호화에 대한 시간 분석 비교 그래프

시스템이지만, 콘텐츠의 일부분을 암호화 시킨 방법으로, 중요한 부분이 암호화가 안되어 있는 단점이 있다. 제안된 암호화 시스템(e)은 부분 암호화 시스템(d)과 동일하게 재생시 다른 블록을 복호화하면서, 시간이 지연되거나 재생이 중단되지 않도록 설계하였다.

4.2 암호화 복호화에 대한 평가

본 논문에서 실험 평가를 하기위해 사용한 비교 DRM 시스템은 Microsoft사의 DRM 시스템과 I-Frame DRM 시스템, 부분 암호화 시스템을 가지고 비교 분석하였다. 실험 데이터 샘플은 18개의 서로 다른 파일크기를 가지고 있는 동영상 데이터를 사용하였다.

(그림 13)과 같이 암호화에 대한 시간을 비교 분석한 결과는 제안한 시스템이 I-Frame DRM 시스템 보다 약 1.12배 향상된 결과를 보이지만, 부분 암호화 시스템에 비교해서는 0.71배로 하향된 결과를 보인다. 그리고 Microsoft DRM 시스템은 암호화시 동영상 콘텐츠를 WMV 파일로 인코딩 작업을 수행한 후 암호화 작업을 하기 때문에 암호화에 대한 시간 분석 비교 그래프에서 제외시켰다.

복호화에 대한 시간 분석을 비교 분석한 그래프는 (그림 12)와 같이 기존의 I-Frame DRM 시스템 보다 약 1.06배 향상되었다. Microsoft사의 DRM 시스템의 경우는 이중버퍼

알고리즘을 사용하지 않고, 재생시 항상 버퍼링에 의존하여 복호화 하기 때문에 전체 복호화 과정이 가장 늦으며, I-Frame DRM 시스템은 암호화 방법과 마찬가지로 GOP 그룹의 모든 헤더를 읽어 I-Frame을 얻어내야 하기 때문에 제안한 시스템보다는 복호화 1.15속도가 느리다. 부분 암호화 시스템은 전체 블록이 암호화 되어 있지 않기 때문에 제안하는 시스템보다는 0.71배 하향된 결과를 보인다.

5. 결 론

본 논문에서는 유·무선을 이용하여 디지털콘텐츠 보호를 위한 해쉬 체인 기법과 세션 상호인증 프로토콜과 암호화 기법 설계에 대하여 제안하였다.

DRM 시스템은 디지털 저작물에 대한 지적재산권에 대한 보호, 유통, 사용이 신뢰할 수 있는 환경에서 이루어질 수 있도록 하는 관리 기술로서 허가받지 않은 사용자로부터 디지털 콘텐츠를 안전하게 보호하여 저작권자의 권리 및 이익을 지속적으로 보호하고 관리하는 기술이다.

그러나 기존의 DRM 시스템은 암호화 알고리즘으로 비밀키 암호 알고리즘을 사용하므로 암호화를 사전에 수행할 수 없으므로 사용자가 디지털콘텐츠 데이터 파일을 다운로드할 때 암호화를 수행하여 다운로드 시간이 많이 소비되며, 사용자에 의하여 비밀키가 노출되면 저작권의 안전을 보장할 수 없는 심각한 문제가 제기되었다. 그러므로 기존의 DRM 시스템에서는 이와 같은 단점을 극복하고자 공개키 암호 알고리즘을 사용하거나 비밀키와 공개키 알고리즘을 혼합하여 암호화를 하는 연구도 진행 중에 있지만 암호화 및 복호화 속도에 미치는 영향이 매우 크므로 만족할만한 결과를 보이지 못하고 있는 실정이다. 사용자에 의한 키의 노출을 막기 위하여 암호화, 복호화 및 저작권 관리에 에이전트를 사용하지만 오프라인 상에서는 기능과 처리의 많은 제약이 있다는 문제점이 제기되었다.

본 논문에서는 디지털 콘텐츠 사용자 인증에 있어서 사용자에 의한 비밀키의 노출을 막기 위하여 해쉬 체인 기법을 사용하여 여러개의 비밀키를 사용하여 전체 데이터를 암호화하는 기법과 세션값을 사용하여 사용자의 상호인증 프로토콜을 제안하였다.

제안한 시스템을 설계하고 구현한 후 성능 평가를 위해 다양한 크기의 비디오 데이터 파일을 이용하여 실험을 수행하였다. 제안한 시스템이 기존 시스템에 비해 클라이언트 시스템에서 비디오 데이터 파일 재생 시 대용량의 디지털콘텐츠에 대해서 복호화 시간을 포함한 지연시간을 현저히 줄일 수 있는 것을 확인하였다.

참 고 문 헌

[1] 김정재 외 2명, "시큐리티 에이전트를 이용한 사용자 인증과 DRM 보안 시스템 설계," 정보처리학회논문지C, Vol.12-C, No.7, pp.973~980, 2005. 12.

[2] 김정재 외 2명, "동영상 데이터 보호를 위한 공유키 풀 기반의 DRM 시스템," 정보처리학회논문지C, Vol.12-C, No.2 pp.183~190, 2005. 4.

[3] 김지홍, 이만영, 류재철, 송유진, 염흥렬, 이임영, 전자상거래 보안기술, 생능출판사, 2001.

[4] Brad Cox, Superdistribution : Objects As Property on the Electronic Frontier, Addision-Wesley, May, 1996.

[5] Sung, J Park, "Copyrights Protection Tech niques," Proceedings International Digital Content Conference, Seoul Korea, Nov., 28-29, 2000.

[6] V.K. Gupta, "Technological Measures of Protection," Proceedings of International Comference on WIPO, Seoul Korea, October, 25-27, 2000.

[7] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography, " IEEE Transac tion on Information Theory, Vol.IT-22, No.6, pp.644-654, November, 1976.

[8] Intertrust : http://www.intertrust.com/main/ overview/drm.html

[9] Joshua Duhl and Susan Kevorkian, "Unde rstanding DRM system: An IDC White paper," IDC, 2001.

[10] Joshua Duhl, "Digital Rights Management : A Definition," IDC 2001.

[11] Microsoft : http://www.microsoft.com/windo ws/windows media/drm.asp

박 찬 길

e-mail : ckpark@hsdu.ac.kr

1991년 서울산업대학교 컴퓨터공학과 (공학사)

1995년 서울산업대학교 컴퓨터공학과 (공학석사)

2006년 숭실대학교 컴퓨터학과(공학박사)

2001~현재 한성디지털대학교 멀티미디어학과 교수

2004~현재 (사)디지털산업정보학회 이사

관심분야 : 네트워크보안, 유비쿼터스, DRM, E-Learning

김 정 재

e-mail : argniss@nate.com

1995년 영동대학교 컴퓨터공학과(공학사)

1999년 숭실대학교 컴퓨터학과(공학석사)

2005년 숭실대학교 컴퓨터학과(공학박사)

2006~현재 (주)RetailTech 수석연구원

관심분야 : 멀티미디어 보안, 멀티미디어 데이터베이스, DRM, RFID

이 경 석

e-mail : kslee@kiet.re.kr
1978년 숭실대학교(학사)
1981년 성균관대학교(석사)
1983년~1986년 Univ. Paris 7 연구소(ITODYS) 연구원
1986년 University Paris 7(박사)
1987년~현재 산업연구원 연구위원
2001년~현재 건국대학교 정보통신대학원 겸임교수
관심분야 : 데이터베이스, 네트워크보안, 정보보안표준, 정보보안알고리즘

전 문 석

e-mail : mjun@computing.ssu.ac.kr
1981년 숭실대학교 전자계산학과(공학사)
1986년 University of Maryland Computer Science(공학석사)
1989년 University of Maryland Computer Science(공학박사)
1989년 3월~7월 Morgan State University 조교수
1989년~1991년 New Mexico State University Physical Science Lab 책임연구원
1991년~현재 숭실대학교 교수
관심분야 : 전자상거래 보안, 인터넷 보안, 멀티미디어 보안, 인증시스템