한국산학기술학회논문지
Vol. 9, No. 1, pp. 108-113, 2008

멀티미디어 콘텐츠 보호를 위한 SOAP을 이용한 키 전송 시스템 설계

이근왕[1*], 김정재[2]

Design of a Key Transfer System Using SOAP for Multimedia Contents Protection

Lee Keun-Wang[1*] and Kim Jeong-Jai[2]

요 약 본 논문에서는 멀티미디어 콘텐츠를 여러개의 블록으로 나누어 끊김이 없는 2중 버퍼 알고리즘을 통해 복호화가 가능하도록 설계하여, 하나의 키가 유출되어도 동영상 전체를 복호화 하지 못하도록 하여 기존의 시스템보다 보안성이 높은 암호화 방법을 제안한다. 또한 시스템간의 상호 인증을 수행할 수 있도록 전자서명과 공개키 알고리즘을 사용하여 콘텐츠 암호화에 사용된 암호화키를 암호화하여 SOAP 메시지를 통해 전송해주는 시스템을 제안한다.

Abstract A proposed system can decrypt each contents block through a double buffer algorithm which can continually buffer contents by dividing a multimedia contents into some blocks and provides more improved method of encryption than existing system by being not capable of decrypting the whole multimedia contents if one key is exposed. Also, using digital signature and public encryption algorithm for mutual authentication between systems, this paper proposes the system which sends and encrypts symmetric keys for contents encryption through SOAP messages.

Key Words : DRM, Asymmetric Key, Key Exchange, SOAP Protocol

1. 서론

인터넷의 확산과 컴퓨터 상호연결성의 증대로 디지털 자원에 대한 유통 환경이 급속히 변화함에 따라 온라인 음악, 동영상, e-Book 등 디지털 콘텐츠의 유통이 활발해지면서 디지털콘텐츠 산업이 미래의 핵심 산업으로 각광을 받았으나 P2P 등의 무차별 공유 서비스로 인해 디지털콘텐츠 산업은 오랜 기간 동안 정체상태를 벗어나지 못하고 있다. 이러한 디지털콘텐츠의 불법복제 기승으로 인해 기존 오프라인 또는 아날로그 콘텐츠의 유통 구조를 장악하던 음반사 또는 영화제작사 등은 심한 타격을 받게 되었으며, 이들 콘텐츠 공급자들은 궁여지책으로 P2P 사이트에 대하여 불법복제 조장이라는 명목으로 소송을 제기하는 한편 인터넷을 통한 어떠한 형태의 디지털콘텐츠 유통 서비스도 강하게 반발하고 있다. 그러나 콘텐츠의 유통 구조가 기존의 오프라인 또는 아날로그 콘텐츠에서 디지털콘텐츠로 전환되어 가는 추세를 피할 수 없다는 인식하에 품질의 손상 없이 복제가 가능한 저작물의 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[1]. 기존 DRM 솔루션들은 암호화에 사용하는 키로 비밀키를 사용하여 사용자가 파일을 다운로드할 때 암호화를 수행하므로 많은 시간이 소요가 되며, 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 있었다.

또한 암호화와 복호화에 사용하는 키가 사용자에 의하여 노출이 된다면 해당 저작물에 대한 보호는 더 이상 보

본 연구는 2007년도 청운대학교 학술연구조성비 지원에 의하여 연구되었음.
[1]청운대학교 멀티미디어학과
*교신저자: 이근왕(kwlee@chungwoon.ac.kr)

장하지 못하는 단점이 있다.

기존의 DRM은 이 문제를 해결하기 위해서 매트릭스 Puzzle 프로토콜을 사용하여 온라인상에서 멀티미디어 저작물에 대한 사용자 인증과 데이터 자체의 암호화를 통해 불법적인 실행을 방지할 수 있는 통합적인 DRM 시스템을 제안한다.

2. 관련연구

2.1 암호화 알고리즘

대칭키 암호 알고리즘은 데이터를 암호화하는 암호화 키와 암호문을 원래의 데이터로 바꿔주는 복호화 키가 같은 알고리즘을 의미한다[5].송신자는 (그림 1)과 같이 전송하고자 하는 평문을 대칭키 Kse(A)와 암호 알고리즘을 통해 암호문으로 변환하여 수신자에게 전송하고, 수신자는 암호화 때 쓰였던 대칭키 Kse(B)와 복호 알고리즘을 사용하여 원래의 평문을 생성한다.

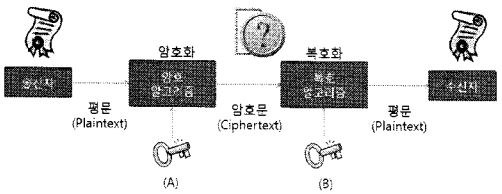


그림 1. 키 사용에 따른 암호화 방법

대칭키 암호화 알고리즘에서의 문제 점인 키 교환 문제점을 해결해 줄 수 있는 암호화 방식이 공개키 암호화 방식이다.

공개키 암호 알고리즘(Public-Key Crypto Algorithm)은 (그림 1)에서 암호화할 때 쓰이는 키(A)와 복호화 하는데 쓰이는 키(B)는 서로 다른 키가 존재하는 알고리즘으로 공개 키 알고리즘이라고도 한다. 개인키로 메시지를 암호화하여 보내게 되면, 송신자의 공개키를 가지고 있는 사람은 누구나 그 내용을 확인할 수 있게 되지만, 수신자는 보낸 메시지가 송신자 본인이라는 것은 누구도 부인할 수가 없게 된다. 이유는 오직 송신자만이 그 자신의 개인키를 알고 있기 때문이며, 이 방법은 서명과 같은 것으로 전송 도중에 제3자의 개입여부를 수신자는 쉽게 알 수가 있는 방법이다[6].

이러한 방법을 전자서명 또는 디지털 서명이라 불리우며 송신자가 평문(M)을 자신의 개인키(KPa)로 암호화한 암호문(S)을 전송한다.

$$S = Envelop(Kpa(M))$$

수신자는 전송받은 암호문(S)을 송신자의 공개키(KUa)로 복호화함으로써 (M)을 얻을 수가 있다.

$$M = Develop(KUa(S))$$

전자서명은 개인키를 소유한 사람에 의해서만 가능하고, 서명의 검증은 누구나 가능하게 된다. 이것이 공개키 암호 알고리즘이 제공하는 인증기법이다.

이러한 공개키 암호 시스템은 대칭키 암호 시스템의 키 관리와 분배의 문제점을 해결해 주고 있다. 공개키 암호 시스템은 전자 상거래에서 보안을 위해 사용하는 SSL이나 IPSec등 보안 프로토콜 등에서 중요한 역할을 하며 대표적인 공개키 암호 알고리즘으로는 RSA암호가 있으며 이 밖에 ElGamal, ECC 등이 있다[7].

2.2 AES암호화 방법

AES 암호 알고리즘은 DES의 안전상의 취약점을 극복하고자 만든 개선된 알고리즘으로 Rijndael 알고리즘이 2000년 10월 최종 AES로 선정되었다. AES 암호 알고리즘의 암호화 연산은 SubByte 연산, ShiftRow 연산, MixColumn 연산, AddRoundKey 연산 등으로 구성된다. (그림 2)는 AES 암호화 알고리즘의 흐름도이다.

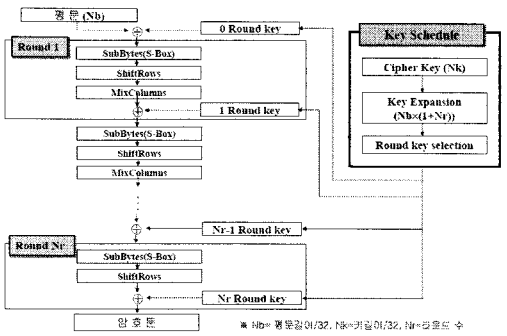


그림 2. AES 알고리즘 흐름도

2.3 PKI 암호화 시스템

공개키 기반 구조는 개방형 네트워크에서 안전한 서비스가 이루어질 수 있도록 통신 정보의 비밀성, 인증, 무결성, 부인방지 등의 기본적인 보안 서비스를 가장 효과적으로 제공하는 기반 구조이다. 공개키 암호 기술의 문제점은 공개키의 가용성을 훼손하는 경우에 발생한다. 공개키의 가용성이란 어느 누구든지 다른 사용자의 공개키가 필요한 경우에 이를 사용할 수 있는 서비스이다.

공개키가 위·변조되지 않았음을 보장하는 문제 즉, 공개키의 무결성을 보장하기 위해 공개키 대신 공개키와 그 공개키의 소유자를 연결하여 주는 인증서를 공개하고, 인증서는 신뢰할 수 있는 제 3자인 인증기관이 자신의 개

인키로 서명하여 공개키를 인증하는 시스템을 PKI 시스템이라 한다.

PKI 시스템은 공개키 암호기술이 안전하게 적용될 수 있는 기반구조로써 공개키와 그 소유자를 연결해 주는 인증서, 키와 인증서를 안전하게 관리해주는 서비스, 그리고 인증서의 유효성 여부를 확인할 수 있는 구조라고 정의한다[6].

2.4 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.

2.4.1 InterTrust의 DRM 시스템

InterTrust사의 DRM 솔루션 특징은 저작물의 보호를 위해서 암호기술과 워터마킹을 사용하며 저작물 사용규칙을 지정하여 사용내역의 수집 및 기록, 과금 처리를 수행하는 것이다. 또한 저작물이 암호화되어 보호되고 있으므로 사용자들 사이에 암호화된 저작물을 주고받을 수 있는 저작물 재분배(SuperDistribution)를 실현하였다[3].

그러나 한개의 키로만 암호화 하므로 키가 유출이 될 경우 더 이상 보호를 받지 못한다는 점과 파일 전체를 암호화하기 때문에 암호화와 복호화 하는데 시간이 다른 시스템보다 오래 걸리는 점과 재생시 전체 복호화가 끝난 후에야 재생이 되는 단점을 가지고 있다.

2.4.2 Microsoft의 DRM 시스템

Microsoft의 DRM 시스템은 저작물 제공자와 소비자들에게 디지털 미디어 파일을 안전하게 분배하는 종단간(end-to-end) DRM 시스템이다[4]. 그러나 Microsoft사의 DRM 시스템의 경우는 자사의 WMV와 WMA의 파일 포맷만을 지원하기 때문에 암호화시 파일 전체를 인코딩하여 암호화하기 때문에 시간이 오래 걸린다.

2.4.3 I-Frame DRM 시스템

I-Frame DRM 시스템은 전체 동영상의 복호화가 끝나기 전에 해당 파일을 재생할 수 있는 이중 버퍼 알고리즘을 사용한다. 그러나 I-Frame을 추출하기 위하여 GOP 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 암호화 된 동영상은 보호를 받지 못한다는 단점과, 재생 시 처음 블록을 복호화 하는데 걸리는 재생 지연시간이 발생한다.

3. 제안시스템 구조

3.1 디지털 콘텐츠 암호화 방법

(그림 3)과 같이 디지털콘텐츠를 암호화하기 전에 원시데이터(Raw Data)를 블록으로 나누어 각각의 블록을 암호화 할 수 있도록 전 처리작업을 수행한다. 전 처리작업 수행시 첫 번째 암호화 블록은 원 데이터가 시작되기 전에 지연시간 만큼을 첫 번째 블록크기로 정하고 두 번째 블록의 크기는 전 블록크기의 100~200% 내에서 블록으로 나누어 처리한다.

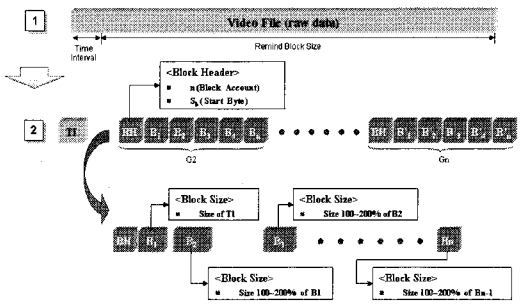


그림 3. 디지털 콘텐츠 블록 분할 기법

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

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

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.

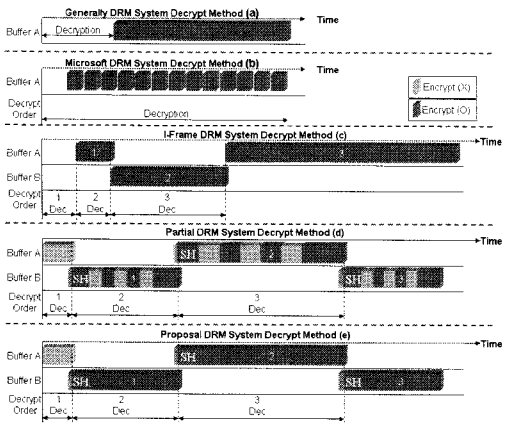


그림 4. 기존 시스템과의 지연 시간에 대한 설계

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 프레임만을 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 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 복호화 하면서, 시간이 지연되거나 재생이 중단되지 않도록 설계하였다.

3.2 디지털 콘텐츠에 사용된 암호화 키 전 방법

3.2.1 인증서 전달구조

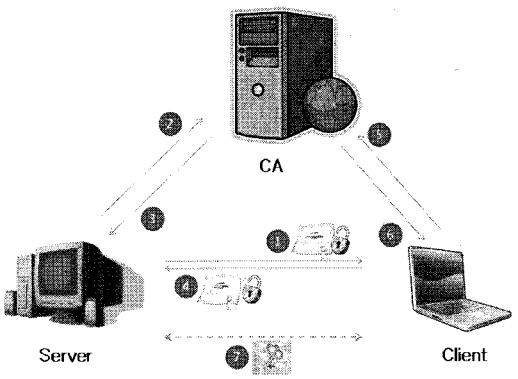


그림 5. 제안하는 시스템의 키 전달 구조

위에서는 Client와 Server간의 암호화 과정을 보여주고 있으며, 과정은 다음과 같다.

① Client 인증서를 Server로 전송
② Client 인증서 상태 검증요청
③ Client 인증서 상태검증
④ Server 인증서를 Client로 전송
⑤ Server 인증서 상태 검증요청
⑥ Server 인증서 상태검증
⑦ 인증완료시 각 블록에 사용된 암호화를 공개키를 이용하여 암호화 데이터 전송은 기본적으로 SOAP을 통해 전송이 된다.

3.2.2 메시지 암호화 과정

본 논문에서 제안하는 콘텐츠에 사용된 암호화 키를 전송하기 위해 시스템간의 인증 및 무결성, 데이터 암호를 모두 할 수 있는 방법을 제시한다.

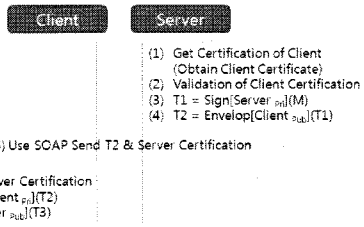


그림 6. 암호화 메시지 전송 방법

Server에서 Client에게 메시지를 전송하기 위해 8번의 단계를 거치며 각 단계별 프로세스는 다음과 같다.

① Client의 인증서를 SOAP 메시지로 획득
② Client의 인증서 상태 검증 (CA에 요청)
③ 콘텐츠에 사용된 암호화 키를 Server의 개인 키로 전자서명 (T1)
④ 단계 ①에서 획득한 Client의 인증서 안에 포함된 공개키를 이용하여 데이터 암호화
⑤ SOAP 프로토콜로 Client에게 암호화 메시지 및 Server 인증서 전송
⑥ Server의 인증서 상태 검증 (CA에게 요청)
⑦ Client의 개인키를 통해 암호화된 메시지 복호화 (원문 메시지 획득)
⑧ 단계 ⑤에서 획득한 Server의 공개키를 통해 메시지의 위변조가 없는지 전자 서명값 검사

(그림 7)에서 암호화하는 시점과 복호화 하는 시점은 모든 데이터가 SOAP이라는 방법으로 서로 전송하기 때문에 암호화한 각각의 데이터를 직렬화를 통해 구성한 다음 MTOM하여 전송을 하며, 복호화 하는 시점은 역직렬화 과정을 통해 데이터를 얻은 후 복호화 하게 된다.

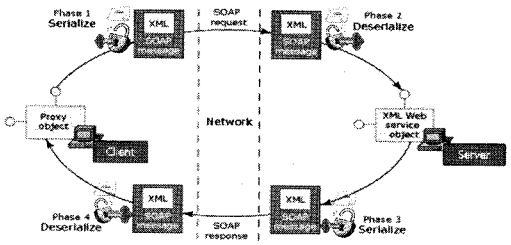


그림 7. 암호화 복호화 시점

4. 성능평가

4.1 안전성에 대한 평가

안정성에 대한 평가는 공개키로 암호화된 디지털콘텐츠 키를 유선망으로 DRM 서버에서 클라이언트로 보내줄 때 암호화 키 유추 가능한 방법에 대해서 서술한다.

스니핑 공격 : SOAP 프로토콜을 사용하여 유선망으로 전송하며 또한 공격자가 만약 공개키로 암호화된 콘텐츠 키를 획득하더라도, 사용자의 개인키가 없기 때문에 스니핑 공격에 대해 안전하다.

스푸핑 및 재전송 공격 : 보내주는 컨텐츠 암호화 키는 전자서명 과정과 타임스템프를 같이 연접하여 사용하기 때문에 스푸핑 및 재전송 공격에 대해 안전하다.

기존 DRM 시스템중 인증서를 사용하지 않는 DRM 시스템의 경우는 콘텐츠를 보호하는 암호화키를 대칭키로 사용하여 전송하기 때문에 서로간의 키 교환 문제가 어려우며, 유선망을 사용하기 때문에 스니핑 공격에 대해 취약하다.

제안한 DRM 시스템은 암호화키를 전송하기 위해 공개키를 사용하여 암호화 한후, 키 전송자의 전자서명 과정을 통해 SOAP 프로토콜을 사용하여 전송되기 때문에 단순히 디지털 콘텐츠 암호화에 사용된 키를 키 조합만으로 인한 키 유출이 매우 힘들며 심지어 여러개의 키로 분할하여 암호화 되어 있기 때문에 몇 개의 키가 유출이 되더라도 전체 동영상에 대해 복호화가 안되기 때문에 기존의 다른 시스템보다 안전하게 보호될 수가 있으며, 스니핑, 스푸핑, 재전송 공격에 강한 특징을 가진다.

4.2 암·복호화에 대한 실험평가

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 8)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.

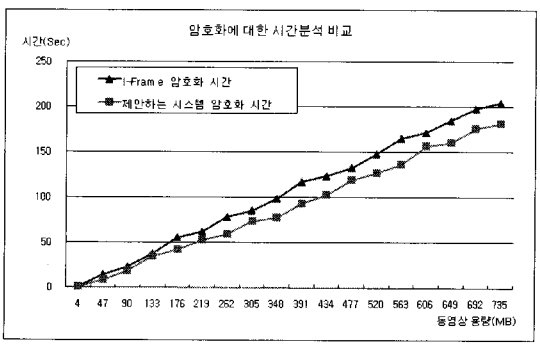


그림 8. 암호화에 대한 시간 분석 비교 그래프

복호화에 대한 시간 분석을 비교 분석한 그래프는 (그

림 9)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.

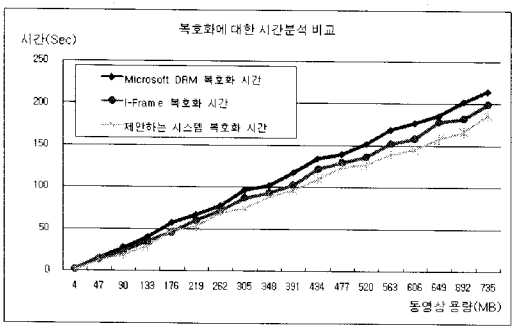


그림 9. 복호화에 대한 시간 분석 비교 그래프

5. 결론

기존의 DRM 시스템은 하나의 대칭키로 암호화하는 것이므로 사용자가 해당 대칭키를 노출시키면 더 이상 해당 저작물에 대한 보호를 보장받지 못하며, 또한 키를 노출시킨 사용자가 누구인지 알 수 없어서 해당 사용자를 추적할 수 있는 방법이 없다.

기존의 암호화 방법에 사용된 대칭키 방식은 키 전송에서 많은 문제점이 발생하였으며, 한 개의 키로만 암호화 되었을 경우 그 키가 유출되었을때 더 이상 보호를 받지 못하는 단점이 있었지만, 본 논문에서는 여러개의 암호화 키를 사용하여 디지털 콘텐츠를 암호화 하고, 그 키들을 공개키 암호화 기법과 전자서명을 통해 SOAP 프로토콜로 전송하는 사용자의 상호인증 프로토콜을 제안하였다.

향후 연구과제로는 연산 수행능력이 현저히 떨어지는 휴대용 기기 및 Off-line 상에서 사용할 수 있는 방법과 기존 시스템 중 콘텐츠 암호화 기법을 연구한 논문과 제안된 키 교환 방법을 결합하여 더욱 우수한 DRM 시스템을 연구할 것이다.

참고문헌

[1] 김정재, "멀티미디어 데이터 보호를 위한 대칭키 암호화 시스템에 관한 연구," 학위논문, 2005.

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

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

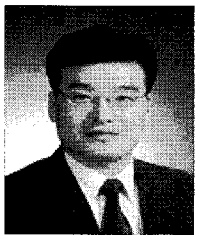
[4] Microsoft : http://www.microsoft.com/windows/ windowsmedia/drm.asp

[5] William Stallings, "Network and Internetwork Security." IEEE PRESS, 1995.

[6] Ron Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of The ACM, Vol.21, No.2, pp.120-126, February 1978.

[7] Gustavus Simmons, Contemporary Cryptology: The Science of Information Integrity, Piscataway, NJ: IEEE Press, 1992.

이 근 왕(Keun-Wang Lee) **[종신회원]**



- 1993년 2월 : 한밭대학교 전자계산학과(공학사)
- 1996년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2000년 2월 : 숭실대학교 컴퓨터학과(공학박사)
- 2001년 ~ 현재 : 청운대학교 멀티미디어학과 조교수

<관심분야>
멀티미디어 프로그래밍, 원격교육, 이동통신, 멀티미디어 응용

김 정 재(Jeong-Jai Kim) **[정회원]**

- 1995년 2월 : 영동대학교 컴퓨터공학과(공학사)
- 1999년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터학과(공학박사)
- 2006년 ~ 현재 : (주) RetailTech 수석 연구원)

<관심분야>
멀티미디어 보안, 멀티미디어 데이터베이스, DRM, RFID