모바일 환경에서 동영상 데이터 보안을 위한 DRM 시스템의 설계

천준호°, 이상훈, 박재표, 정용득, 전문석
숭실대학교 대학원 컴퓨터학과
opendream@hanmail.net, iam@leesanghun.pe.kr, pjerry@dreamwiz.com
jungyd@kotra.or.kr, mjun@computing.ssu.ac.kr

Design of Digital Right Management System for Multimedia Data on Mobile Enviroment

Junho Choun, Sanghun Lee, Jaepyo Park, Yongdeok Jung, MoonSeog Jun
Dept. of Computing in Soongsil Univ.

요 약

무선 인터넷의 보급과 맞물려 모바일 컴퓨팅 환경이 구축됨에 따라 PDA와 같은 소형의 모바일 장비에 최적화된 디지털 컨텐츠의 제작 및 배포가 활발해지고 있으며 불법적인 디지털 컨텐츠의 이용 또한 이에 비례하고 있다. 그러나 유선환경에 기반한 기존의 DRM 시스템은 상대적으로 속도와 표현능력이 떨어지는 모바일 환경에는 적합하지 않으며 현재 연구·개발된 모바일 환경에서의 DRM 시스템은 음악, 문서, 이미지에 국한되어 있어 동영상과 암호화와 같은 높은 연산 능력을 요구하는 부분의 개발과 연구는 초기 단계에 머물러 있다.

본 논문에서는 모바일 환경에 적합하도록 적은 연산 능력으로도 기존의 DRM 시스템에 준하는 보안 강도를 갖을 수 있도록 동영상의 부분 암호화 방식과 공유키 풀 기반의 인증 방법을 사용하는 DRM 시스템을 설계·제안한다.

1. 서 론

최근 수년간 초고속 인터넷의 대중화는 정보화 사회를 이끌어 가는 원동력이 되었지만 소프트웨어의 대량 불법 복제라는 문제를 함께 가져왔고 저작권 보호와 디지털 컨텐츠의 새로운 유통 구조를 위해 DRM(Digital Right Management)이 사용되었다.

DRM은 디지털 컨텐츠를 보호하고 관리하는 것으로서 디지털 워터마킹, 암호화, 접근제어와 같은 저작권 보호 관련 기술로 불법 복제에 대응하고 XrML, DOI와 같은 저작권 관리 기술을 사용하여 디지털 컨텐츠의 제작과 유통까지의 전과정을 포괄적으로 관리하는 기술이다[1]. 이러한 DRM 기술은 유선환경에서 저작권 문제를 해결하기 위해 사용되어 왔으나 무선 인터넷 환경에서 PDA와 같이 작은 화면과 해상도, 낮은 CPU속도와 메모리를 가진 모바일 기기에 그대로 적용하기 어렵다.

현재 Microsoft, InterTrust등의 업체가 모바일 환경에서의 DRM을 시도하고 있으나 상대적으로 적은 연산 능력을 요구하는 이미지, 문서에 대한 것뿐 음악이나 동영상과 같은 멀티미디어 데이터에 대한 솔루션은 개발 초기화 단계이다[2,3].

본 논문에서는 PDA와 같은 모바일 장비의 하드웨어적 한계 상황에서도 유선 환경에 근접한 보안 강도를 유지하는 DRM 시스템을 제안하고자 한다. PDA는 운영체제별로 서로 다른 파일 포맷을 사용하므로 PC를 통하지 않고는 타기종 사이에 직접 호환되지 않는다.

현재 Palm사의 PalmOS와 Microsoft사의 PocketPC로 양분되어 있으나 본 논문에서는 멀티미디어 지원 능력과 무선 인터넷 사용의 용이성을 고려하여 PocketPC를 타겟 플랫폼으로 정하였다.

본 논문의 구성으로, 2장에서는 DRM의 요소 기술에 대해 언급하고, 3장에서는 무선 인터넷 환경에 적합한 암호화 방식인 부분 암호화와 인증을 위한 공유키 풀을 이용한 암호화 방식을 설계·제안하며, 4장에서 본 논문이 갖는 의미와 향후 발전 발향을 기술한다.

2. 관련 연구

2.1 저작권 관리를 위한 기술

저작권 관리 기술이란 온라인 환경에서 디지털 컨텐츠

의 제작자 및 배포자의 저작권을 지속적으로 관리하는 기술을 의미한다. 이러한 저작권 관리 기술에는 각각의 디지털 컨텐츠를 고유하게 식별하게 해주는 컨텐츠 저작권 등록 관리 기술(DOI, Digital Object Identifier)과 디지털 컨텐츠에 저작권을 명세하고 관리 시스템을 효과적으로 구축하기 위한 XrML(eXtensible Right Markup Language)가 있다.

- Digital Object Identifier : DOI는 디지털 컨텐츠나 웹 페이지의 인터넷 주소가 변경되더라도 사용자가 새로운 주소로 다시 찾아 갈 수 있도록 영구적으로 부여된 식별자이다. DOI 시스템은 본질적으로, 중앙의 관리자 프로그램이 디지털 컨텐츠나 웹페이지의 인터넷 주소를 언제나 유지할 수 있게 하는 것이다[4].
- eXtensible Markup Language : XrML은 권리를 명시하는 언어로써 디지털 컨텐츠와 그에 따른 서비스들을 사용할 수 있는 권리와 조건들을 명시해준다[5].

2.2 저작권 보호를 위한 기술

- Encryption Algorithms : 사용하는 키에 따라 대칭형과 비대칭형으로 나눌 수 있다. 대칭형 암호화 알고리즘은 동일한 키로 암·복호화를 수행하며 비대칭형에 비해 빠른 속도를 갖지만 최초의 키 교환시 보안에 취약해진다. 이를 보완하기 위해 데이터 전체를 비대칭형 암호화 알고리즘으로 암호화를 수행하면 대칭형에 비해 수배의 시간이 소요되므로 비대칭형 암호화 알고리즘으로 대칭키 혹은 메시지 다이제스트만을 암호화하는 전자봉투(Digital Envelope)나 전자서명(Digital Signature) 형태로 이용한다[6].
- Digital Watermarking : 디지털 컨텐츠 내에 저작자 정보 또는 이용자 정보를 분리 할 수 없는 방법으로서 부가정보를 일정한 패턴이나 코드로 바꾸어 디지털 컨텐츠에 비가시적으로 삽입하여 저작권을 보호하는 방법으로 동영상, 문서, 이미지, 음악자료 등에 DOI, XrML 정보를 삽입하여 사용 할 수 있다[7].

3. 모바일 동영상 보안시스템 설계

3.1 시스템의 개요

본 논문에서 설계 및 제안한 DRM 시스템은 (그림 2)와 같이USER, CA, License/Storage Server로 구성된다.

- USER : PDA를 사용하는 사용자
- CA : USER에게 인증서(Cert_u)를 발급하며 3.3의 공유키 풀을 생성하고 LS의 인증서 검증 요청에 응답한다.
- License Server(LS) : 사용자 인증과 CA, USER, SS의 중계를 담당한다.
- Storage Server(SS) : 동영상의 암호화와 저장을 담당한다.

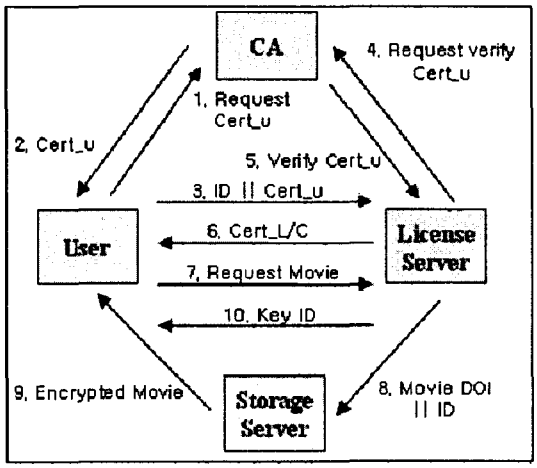


그림1. 제안된 DRM 시스템의 개요

USER와 CA 사이에서 인증서(Cert_u) 요청과 발급이 정상적으로 진행되면(1,2) USER는 LS에게 접근시 자신의 ID와 Cert_u를 넘겨주고(3) LS는 CA에 질의하여 정당한 사용자인지 여부를 판단한 후(4,5) USER에게 공유키 풀의 키 리스트를 넘겨준다(6). USER가 동영상을 신청하면(7) LS는 해당 동영상의 DOI와 USER의 ID를 SS에게 알려주어서 USER에게 암호화된 동영상을 배포하게 한다(8,9). LS는 최종적으로 동영상의 복호화에 필요한 Key_ID를 USER에게 알여줌으로서 일련의 과정을 종료한다.

3.2 동영상 부분 암호화 모듈 설계

데스크탑에 비해 상대적으로 연산 능력이 떨어지는 PDA에서 전체 암호화된 동영상을 복호화 할 경우 많은 시간이 소요되므로 (그림 2)에 표시된 것과 같이 동영상의 헤더 부분과 컨텐츠 부분의 일부 프레임만을 암호화하는 부분 암호화를 통해 복호화 속도를 향상시킨다.

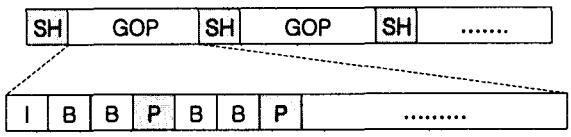
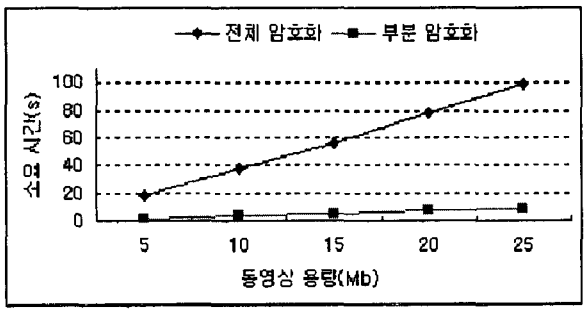


그림2. 동영상 데이터의 부분 암호화

시퀀스 헤더(SH)는 화면의 크기, 화소의 종횡비, 비트율등의 정보를 담고 있으며, GOP(Group of Picture) 내부의 P프레임은 P프레임 바로 이전의 I프레임이나 P프레임을 참조하여 그 화면의 변화를 예측하는 프레임이다[8]. 따라서 전체 동영상을 암호화 하지 않고 SH와 P프레임을 암호화하는 것만으로도 키가 없는 사용자는 동영상을 정상적으로 재생 할 수 없게 되며, 실제로 AES 암호화 알고리즘으로 암호화된 동영상을 PDA상에서 복호화하는데 소요되는 시간도 (표1)과 같이 단축된다.

표1. PDA상에서 AES 알고리즘의 복호화 소요시간 비교



3.3 인증 모듈 설계

(a) $Ks = Ks1 \mid Ks2 \mid Ks3 \mid \cdots \mid Ksk$

(b) $a1^0, a1^1, a1^2, \cdots, a1^{2^{\frac{n}{k}}-1}, \cdots, ak^0, ak^1, ak^2, \cdots, ak^{2^{\frac{n}{k}}-1}$

(c) $Kp = a1^{b_1} \mid a2^{b_2} \mid a3^{b_3} \mid \cdots \mid ak^{b_k}$

(d) $b_1 \mid b_2 \mid b_3 \mid \cdots \mid b_k$

(e) $a'i^F = Ks_i \text{ xor } ai^F$

공유 키 풀을 구성하기 위해서 동영상의 비밀키 Ks를 사용하여 암호화하여 k개의 비트열로 나누고(a), 이를 이용하여 $k*2^{\frac{n}{k}}$개의 비트로 구성된 공유 키 풀을 생성한다(b). 각 사용자 들이 사용 할 키 K_p는 k비트로 이루어진 비트열의 집합이다(c). b_i는 사용자 인증서의 공개키에서 추출하는 것으로 공유키 풀에서 사용자의 개인용 키를 결정하는 값이다(d). 복호화에 사용될 개인키가 사용자의 공개키에 의해 결정되므로 모든 사용자는 자신만의 고유한 키를 사용하게된다.

공유키 풀이 생성되면 비밀키 Ks를 암호화하기 위하여 공유 키 풀의 $2^{\frac{n}{k}}$개의 비트인 ai^0, ai^1, $ai^2, \cdots, ai^{2^{\frac{n}{k}-1}}$에 각각 Ks_i와 비트 단위의 배타적 논리합을 하여 최종적인 공유키 풀을 얻는다(e).

4. 결론

최근에 출시되는 모바일 장비의 하드웨어의 성능이 날로 향상되고 있지만 유선환경과 대등한 성능을 기대하기는 어렵기 때문에 본 논문에서는 보안 요소를 간소화하여 모바일 장비의 하드웨어적 한계를 고려하면서도 유선환경과 대등한 보안 강도를 유지하려 했다. 동영상의 부분 암호화 방식을 통해 전체 암호화를 하지 않으면서도 그에 준하는 보안 강도로 부적절한 사용자의 디지털 컨텐츠 사용을 막고자 했으며 공유 키 풀 방식을 사용함으로서 키 생성에 소요되는 시간을 단축하였다.

향후 연구과제로는 부분 암호화 방식에서 암호화 하는 프레임의 수를 늘리거나 암호화 하고자 하는 프레임을 임의로 추출하는 방법으로 암호화의 비도를 향상시키고자 한다.

한편 무선 인터넷 사용시 배터리 가용량이 급격히 줄어드는 점을 감안하여 Super Distribution[9,10]을 통해 미리 다운 받은 암호화된 동영상에 라이센스만을 무선으로 발급 받아 사용하는 방법을 연구하고자 한다.

5. 참고문헌

[1] Joshua, D. Susan, K., "Understanding DRM System" IDC White Paper, IDC, 2001.

[2] Intertrust : intertrust.com/main/overview/drm.html

[3] Microsift : microsoft.com/windows/windowsmwdia/drm.asp

[4] James Daziel, "DOI in DRM environment", DOI EPICS Project White Paper.

[5] eXtensible right markup Language (XrML) 2.0 Specification, http://www.xrml.org.

[6] 전문석외, "정보이론 및 PKI", 미래컴, 2003

[7] 강석준. 배태면, 노용만, 인소란, 유비쿼터스 환경에서 컨텐츠 적응변환을 위한 워터마킹 시스템, 정보과학회 춘계학술대회, 2004.

[8] MPEG-21 Part 4 : MPEG-21 IPMP Ver.5, Moving Picture Experts Group, 2002.

[9] Qiong Liu외, "Digital Right Management for Contents Distribution", Australian Computer Society Workshop 2003.

[10] 김후종, 나승원, "무선 인터넷 환경에서 디지털 컨텐츠 저작권 보호를 위한 모바일 보안 시스템의 설계 및 구현", 한국정보처리학회 논문지, 2003.