무선 인터넷 환경에서 디지털 컨텐츠 저작권 보호를 위한 모바일 보안 시스템의 설계 및 구현

김 후 종† · 나 승 원††

요 약

무선 인터넷의 활성화와 함께 다양한 형태를 가진 디지털 컨텐츠의 유통이 활발해지고 있다. 이에 따라 불법 복제를 통한 컨텐츠 유통을 방지하고 사용자에게 적절한 컨텐츠의 이용 권리를 부여하기 위하여 모바일 환경에 기반한 디지털 저작 관리(DRM : Digital Rights Management) 시스템의 필요성이 대두 되고있다. 본 논문에서는 모바일 환경에서 유통되는 디지털 컨텐츠의 저작권을 보호하기 위한 보안 시스템을 제안하였다. 본 시스템은 무선 환경에서 적용되는 모바일 전용 DRM 설계 방법을 제안하는 것을 목적으로 한다. 특히 본 시스템은 모바일 디바이스의 복호화 처리 능력을 고려하여 부분 암호화 방법을 채택하였다. 이에 대하여 각 컨텐츠 암호화 방법(전체 암호화와 부분 암호화)의 성능을 비교, 평가하고 현재의 무선 디바이스에서 적합한 DRM 시스템은 부분 암호화의 모듈을 적용한 시스템임을 검증하였다. 본 논문에서 제안한 모바일 DRM 시스템은 무선 인터넷 환경에서 유통되는 컨텐츠를 보호하는데 큰 효과를 제공할 수 있다.

Design and Implementation of Mobile Security System for Digital contents Rights Protection in Wireless Internet Environment

Hoojong Kim† · Seungwon Na††

ABSTRACT

As wireless Internet spreads widely, circulation of various types of digital contents becomes active. Therefore, it is necessary to make a mobile-based DRM (Digital Rights Management) system to protect digital contents from illegal reproduction and to give proper rights to contents users. In this paper, we present a mobile security system, which protects the copyright for digital contents offered throughout the mobile environment. Our security system is focused on presenting mobile-based DRM architecture. Especially, considering mobile device's decrypting power, we adopted partial encryption scheme. For this, we compared and evaluated the performance of each contents encryption scheme (the entire encryption scheme and the partial encryption scheme) and proved that a proper DRM system for current wireless devices is the partial encryption system. Our mobile DRM system can be very efficient to protect contents on the wireless Internet environment.

키워드 : 모바일 보안(Mobile Security), 디지털 저작 관리(DRM), PDA, 부분 암호(Partial Encryption)

1. 서 론

무선 인터넷 사용자의 증가와 함께 컨텐츠 시장이 활성화되면서 다양한 컨텐츠가 무선 인터넷 환경에서 사용 가능한 디지털 형태로 제작되어, 활발하게 유통되고 있다. 이 과정에서 디지털 컨텐츠의 불법 유통으로 인한 저작권 침해의 문제가 발생하고 있어서 무선 멀티미디어 유통 산업의 발달에 심각한 피해가 우려되고 있다. 이와 같은 문제의 해결을 위해서 디지털 저작관리(DRM : Digital Rights Management)기술의 필요성이 대두되고 있다[4, 9]. DRM기술은 컨텐츠를 보호하고, 관리하는 시스템으로써 다양한 비즈니스 모델을 지원하고 암호화, 워터마킹 등 보안 기술을 사용하여 불법 사용을 억제하고, 사용자 인증이나 관리 기능을 제공할 수 있는 기술이다[2].

현재, 정보보호 경우는 암호화 기술, 디지털 워터마킹 기술, 침입탐지 기술 등에 대한 연구들이 수행되고 있다[8, 10]. 디지털 저작관리 및 보호를 위한 기반 기술의 식별자 분류 방법으로는 DOI(Digital Object Identifier) 분류 체계가 있고 XrML(extensible right Markup Language)과 Dublin Core 등 저작권 및 사용권에 대한 메타 데이터를 관리하기위한 언어가 있다[17]. DRM 솔루션의 경우 Microsoft, InterTrust,

† 정 회 원 : SK텔레콤 Platform 연구원 Terminal 개발팀장
†† 준 회 원 : SK텔레콤 Platform 연구원 Terminal 개발팀 과장
논문접수 : 2003년 7월 22일, 심사완료 : 2003년 10월 20일

ContentGuard 등의 업체가 주로 다양한 형태의 유선 DRM 솔루션을 제공하고 있으나, 무선 인터넷 컨텐츠를 보호하기 위한 DRM 솔루션은 개발 초기의 단계이다.

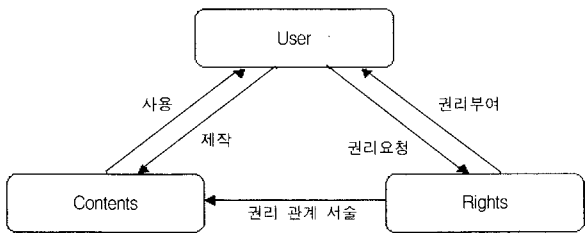
본 논문에서는 무선 인터넷 환경에서 제공되는 디지털 컨텐츠(그림친구, 벨소리, 전자북, 동영상 파일, 게임)등을 보호하기 위한 모바일 보안 시스템을 제안하고자 한다. 제안하는 시스템의 특징은 무선 디바이스에서 원활히 수행되기 위한 부분 암호화 방법으로 전체 암호화와 부분 암호화의 성능 비교를 통해서 부분 암호화 성능을 구체화 하였다.

본 논문의 구성으로, 2장에서는 일반적인 DRM 기술과 보안 알고리즘에 대해서 기술하였고, 3장에서는 무선 인터넷 환경에 적합한 DRM을 전체 암호화와 부분 암호화의 비교 방법으로 제안하였다. 4장에서는 프로토타입의 구현으로 성능 분석과 실험 결과를 제시하였다. 마지막으로 5장에서는 결론과 향후의 연구 방향에 대해서 기술하였다.

2. 관련 연구

2.1 DRM 기술 현황

인터넷에서 유통되고 있는 디지털 컨텐츠의 저작권을 보호하기 위한 기술로써 DRM과 디지털 워터마킹(Didital Watermarking)기술 등이 적용되고 있다[8]. 워터마킹 기술은 소극적인 형태의 저작권 추적 기술이지만, 변조 등 각종 공격에 취약하기 때문에 컨텐츠의 판매등 적극적인 권리 행사를 위해서는 적합하지 못하다는 의견이다. 반면에 DRM 기술은 컨텐츠의 저작권 소유자, 사용권 소유자, 사용 기간, 요금, 사용횟수 등 보다 적극적이고 다양한 정보를 다룰 수 있고 강력한 복제 방지 기능을 지니고 있어서 최근 암호화를 위한 기술로써 웹 환경에 활발하게 적용되고 있다. 일반적으로 DRM의 구성 요소는 (그림 1)과 같다.



(그림 1) DRM의 구성요소

사용자(User)는 원하는 컨텐츠(Contents)를 이용하기 위해서 컨텐츠 사용 권한에 대한 권리(Rights)를 부여 받는다. 이때 권리의 의미는 컨텐츠에 관계된 소유, 사용, 변조, 배포등 여러 가지 권리 관계를 서술하고 있다[17]. 이 같은 요소를 바탕으로 DRM 기술은 여러 기구에서의 표준화 작업이 이루어지고 있으며 DRM 서비스를 제공할 수 있는 DRM 솔루션의 연구도 활발히 이루어지고 있다.

2.1.1 DRM 기술 표준화 작업

DRM 기술의 표준화 작업은 여러 기구에서 진행되고 있다. 전자책, 오디오, 비디오 컨텐츠 등에 대한 표준화 작업뿐 아니라 권리 표현언어(Right Expression Language)에 대한 표준화 작업도 진행되고 있다. 대표적인 표준화 작업은 OeBF, MPEG-21, XrML등이 있으며 다음과 같다[13].

첫째 : OeBF(Open eBook Standard Forum)는 전자책의 표준을 제정하기 위한 국제 표준조직으로 Microsoft를 중심으로 Intertrust, Adobe등이 참여하고 있다.

둘째 : MPEG-21은 오디오, 비디오, 그래픽 등 멀티미디어를 비롯하여 전자책, 방송, 디지털 시네마 등 거의 대부분의 디지털 컨텐츠를 제공할 수 있는 멀티미디어 프레임워크의 표준을 지정하기 위하여 만들어졌다[6]. MPEG-21은 멀티미디어 프레임워크를 7개의 요소로 분류하여 각각의 요소에 대하여 표준화 작업을 시행하고 있다. 이 중에서 DRM과 관계된 부분이 IPMP (Intellectual Property Management and Protection)이며 2001년 표준화 작업을 시작하여 2005년에 완성할 예정이다.

셋째 : XrML(eXtensible rule Markup Language)은 컨텐츠를 배포하기 위해서는 컨텐츠의 소유자, 사용자, 사용권리 등 다양한 정보를 서술하기 위한 언어가 필요하여 가장 널리 쓰이고 있는 언어가 XrML이다[1].

2.1.2 DRM 솔루션 현황

DRM의 필요성이 증대되면서 컨텐츠를 서비스하기 위해서 단순한 표준이 아닌 상업화된 DRM 서비스 시스템의 구축이 필요하게 되었다. 이를 위하여 여러 회사에서는 서버 및 클라이언트를 제어할 수 있는 통합된 DRM 솔루션을 개발하고 있다. 첫째, Microsoft DRM은 Windows Media Player를 기반으로 재생되는 컨텐츠에 적용되는 DRM 시스템이다. Microsoft DRM은 라이센스와 미디어가 분리 배포되며, 라이센스 조건의 변경이 쉽고 미리보기 제한, 휴대용 SDMI 장치에 대한 전송 제한 등 세부 기능을 포함하며 DRM 관리용 서버 패키지도 함께 제공된다[12].

둘째, InterTrust DRM은 InterTrust에서 윈도우 및 솔라리스 계열을 대상으로 암호화 및 워터마킹이 가능한 DRM 솔루션을 제공하고 있는 시스템이다. 사용 정보의 권리를 서술하기 위하여 XrML을 사용하지만, 비 공개되어서 일반인들은 해당 정보를 알 수 없는 특징이 있다.

셋째, ContentGuard DRM은 ContentGuard에서 제공하는 DRM 솔루션으로 윈도우 및 솔라리스 계열을 지원하고 암호화 및 워터마킹이 모두가 가능하다. 사용정보 권리 서술

을 위하여 XrML을 사용하며 공개된 내용이므로 일반인도 정보를 알 수 있다.

2.2 암호화 알고리즘

DRM 컨텐츠의 암호화 알고리즘은 생성하거나 데이터 변조 여부를 측정하기 위한 메시지 다이제스트를 만들 때 사용하는 해싱(Hashing) 알고리즘과 디지털 컨텐츠 암호화를 위한 알고리즘, 그리고 키 전송 및 전자서명 등을 위한 암호화 알고리즘등 세가지 형태로 나뉘며, 데이터를 전송하기 위한 보안 전송 프로토콜로는 대표적으로 SSL(Secured Socket Layer), TLS(Transport Layer Security) 등의 방식이 이용되고 있다[3, 16].

2.2.1 해싱 알고리즘

해싱 알고리즘은 임의의 길이를 가지고 있는 메시지를 받아들여 고정된 길이의 출력 값으로 바꿔주는 알고리즘이다. 해싱을 수행하는 함수를 해시 함수라고 부르고 해싱의 결과로 나온 값을 해시 값 혹은 메시지 다이제스트라 한다. "해시 함수의 기본 조건은 동일한 해시 값을 갖는 두 개의 서로 다른 메시지는 존재하지 않는다"는 특징이 있다. 암호화 알고리즘과 달리 해시 값을 이용하여 원본 데이터를 알아내는 것은 불가능하지만, 제 3자에 의하여 데이터가 변조되었는지 여부를 파악하는데 유용하게 사용할 수 있다. 이러한 성격 때문에 해싱 알고리즘을 단 방향(One-Way) 알고리즘이라고 부른다.

2.2.2 컨텐츠 암호화 알고리즘

컨텐츠를 암호화하는 방식으로는 DES나 AES등의 대칭키 암호화 알고리즘을 사용하게 된다. 대칭 키 암호화 알고리즘은 동일한 키를 이용하여 암호화 및 복호화를 수행할 수 있고 비교적 빠른 속도를 가지고 있는 특징이 있다.

DES(Digital Encryption Standard)는 대칭 키 알고리즘의 대표적인 방식으로 56비트의 키를 사용하여 메시지를 암호화하는 블록 암호 알고리즘의 일종이다. 암호화와 복호화를 하나의 대규모 집적 회로(LSI)로 고속 처리할 수 있도록 개발되어있다.

AES(Advanced Encryption Standard)는 DES의 작은 키 값으로 보안 문제가 발생되어 탄생된 것으로써 DES와 마찬가지로 대칭키 암호화 알고리즘에 속하며 보안 정도에 따라 128, 192, 256비트의 세가지 키를 사용하여 56비트인 DES보다 훨씬 더 안전한 기능을 제공하는 특징이 있다.

2.2.3 키 전송 및 전자 서명 알고리즘

대칭키 알고리즘으로 암호화된 컨텐츠를 전송하는 과정에서 키를 안전하게 전송하고 컨텐츠의 내용이 변조되었는지 여부를 파악하기 위하여 공개키 알고리즘에 기반한 암호화 시스템이 도입되었다. 공개키 알고리즘은 공개키와 비밀키등 두 개의 키를 기반으로 적용되어 있다.

공개키는 임의의 사람에게 접근이 가능한 키이고 비밀키는 본인만 접근이 가능한 키로 특정한 사람의 공개키로 암호화된 내용은 그 사람이 지닌 비밀 키로만 해독할 수 있다. 이러한 특성 때문에 공개키 암호화 알고리즘은 대칭 키의 교환 및 전자서명 등에 응용되고 있다. 가장 대표적인 공개키 암호화 알고리즘으로는 RSA(R. Rivest, A. Shamir, L. Adelman), DSS(Digital Signature Standard) 등이 있다.

2.3 무선 인터넷에서의 보안 연구

2.3.1 무선 인터넷 보안 현황

유선 인터넷의 경우에는 일반적으로 Telnet, Ftp등과 같이 원격지의 시스템을 사용하거나 원격지에 있는 자료를 사용하는 것으로 시작하여 현재까지도 침입차단 시스템, 침입탐지 시스템과 같은 네트워크 시스템 등을 대상으로 보안이 적용되고 있다. 반면에, 무선 인터넷의 경우에는 모바일 커머스, 모바일 뱅킹, 모바일 트레이딩과 같은 전송되는 데이터에 대한 보안 서비스가 먼저 요구되고 있다. 현재 무선 인터넷의 보안은 크게 W-PKI(Wireless Public Key Infrastructure), M-VPN(Mobile Virtual Private Network)시스템으로 적용되고 있다. 주요 특징은 <표 1>과 같다.

〈표 1〉 무선 인터넷 보안 규격

항 목	W-PKI	M-VPN
적용 응용 프로그램	불특정 다수에게 서비스하는 보안	특정 다수에게 서비스하는 보안
보안 측면	네트워크 보안 취약	네트워크와 전송데이터의 완벽한 보안 서비스
적용 규모면	대규모의 응용 서비스	특정 사용자를 위한 규모의 응용 서비스
보안 정책 측면	신규 보안 정책 설정 필요	기존의 보안 정책 적용
신규시스템 측면	W-PKI 신규 시스템 필요	기존의 VPN 기술 이용 (기술적 이해 용이)
응용 프로그램 관계	응용프로그램마다 연동 필요	응용 프로그램과 독립적
비용 측면	고 가	중 가

2.3.2 Mobile DRM 솔루션 현황

Mobile DRM 솔루션은 모바일 디바이스의 성능 및 망 속도 제한 등의 이유로 현재는 활성화 되어 있지는 않다. 단말 제조사에서 다운 받은 컨텐츠의 불법 복제가 단말기에서 불가능하도록 사전방지(forward-lock)를 거는 정도이다. 국내의 이동통신 업체인 S사에서도 무선 컨텐츠 DRM에 대한 상용화 서비스를 2003년말부터 시작하는 수준이다.

그러나 미래의 무선 컨텐츠의 산업 확대를 대비하여 OMA

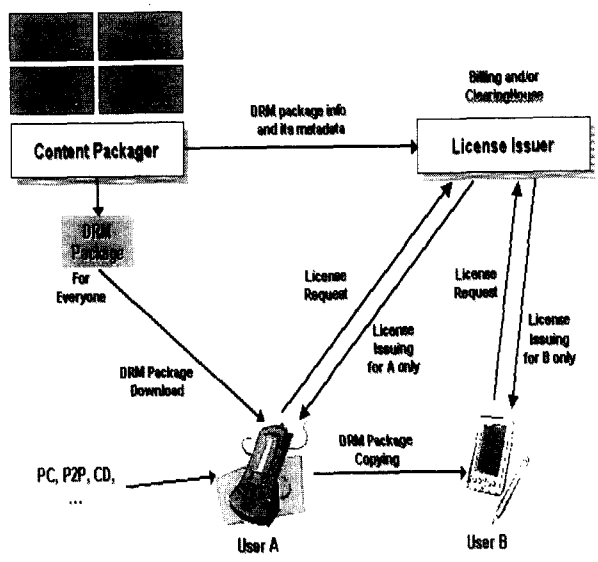
(Open Mobile Alliances)를 통해 표준화 작업이 진행되고 있다. OMA MDRM version 1.0은 사전방지가 걸려있지 않은 단말기에서의 컨텐츠 불법 복제를 방지하고, 컨텐츠 제작자가 안전하게 컨텐츠를 배포할 수 있게 한다는 두 가지 목적을 지닌다[5]. OMA DRM은 XML에 기반한 디지털 저작권 언어인 ODRL(Open Digital Rights Language)을 적용하여 DRM 방식을 지원한다[7]. OMA는 2002년 9월 Version 1.0의 OMA MDRM 스펙을 최종 승인하였고 보다 확장된 기능을 제공하는 새로운 스펙을 제정하기 위한 작업을 진행하고 있다.

3. 모바일 컨텐츠 보안시스템 설계

본 절에서는 무선 이동 단말기인 PDA(Personal Digital Assistants)를 대상으로 디지털 컨텐츠 사용 권리에 대한 보안 시스템의 설계를 제안하고자 한다. 특히, 디바이스에서 복호화 처리 능력을 고려하여, 부분 암호화를 적용하였으며, 이를 검증하기 위해서 컨텐츠의 전체 암호화와 부분 암호화 방법을 비교하여 디바이스 처리 성능에 적합한 컨텐츠 보안 시스템의 설계 방법을 제안하였다.

3.1 시스템의 개요

본 시스템은 휴대용 정보 단말인 PDA(Personal Digital Assistants)에서 무선 인터넷 사용시 유통되고 있는 디지털 컨텐츠를 보호하기 위한 디지털 저작권 관리 시스템(DRM : Digital Rights Management)의 설계 방법을 제안하고자 한다. PDA에서 DRM을 적용하는 디지털 컨텐츠의 형태는 주로 그림친구, 벨소리, 동영상 파일, 전자북, 기타응용 프로그램을 대상으로 한다. 본 논문에서는 이미지 포맷 형식을 대상 DRM 컨텐츠로 설계하였으며 전체적인 시스템 구성도는 (그림 2)와 같다.



(그림 2) 모바일 DRM의 시스템 구성도

(그림 2)에서 DRM 시스템의 구성 요소는 컨텐츠 서버(CS : Content Server), 라이센스 서버(LIS : License Issuing Server), 이동 단말기(PDA : Personal Digital Assistant)등 세 가지로 구성된다.

첫째 : 컨텐츠 서버는 원본 컨텐츠를 컨텐츠 제작자로부터 등록 받아 컨텐츠 DRM 패키저(Packager)를 이용하여 암호화 패키징을 수행한다. 즉, 원본 컨텐츠를 암호화하고 단말기에서 패키지를 원래 컨텐츠로 복구할 때 요구될 정보들을 패키지 헤더로 구성하는 일을 수행한다. 또한 DRM 패키징시에 컨텐츠 암호화 키(CEK : Contents Encryption Key)를 해당 DRM 컨텐츠의 라이센스안에 포함하여 PDA로 내려 주기 위해서 라이센스 서버에 CEK와 DRM 패키징 관련 정보를 등록하는 기능도 수행한다. DRM 컨텐츠는 컨텐츠 서버에 있는 로컬 DB에 저장되며 라이센스 서버로부터 라이센스를 발급 받아 다운로드 서버로 DRM 컨텐츠와 라이센스를 전달하여 사용자에게 서비스 되어진다.

둘째 : 라이센스 서버는 사용자가 DRM 패키징 된 컨텐츠를 적법한 방법으로 사용할 수 있도록 라이센스를 발급하고 관리하는 기능을 한다. 라이센스에는 DRM 컨텐츠의 암호화 키와 PDA 사용자가 구입한 권리 제약사항 등의 정보가 암호화 코드값으로 표현되어 있다.

셋째 : 이동 단말기인 PDA에는 사용자가 구입한 DRM 컨텐츠를 활용할 수 있도록 라이센스를 확인하고 라이센스의 사용 권리 정보에 준하여, DRM 컨텐츠를 복호화하고 컨텐츠 플레이어 및 뷰어에게 원본 컨텐츠를 전달해주는 DRM 클라이언트 모듈이 포함되어 있다. 해당 DRM 패키지에 대한 라이센스가 없거나 권리 제약 사항이 무효화된 라이센스를 보유한 경우는 사용이 불가하다.

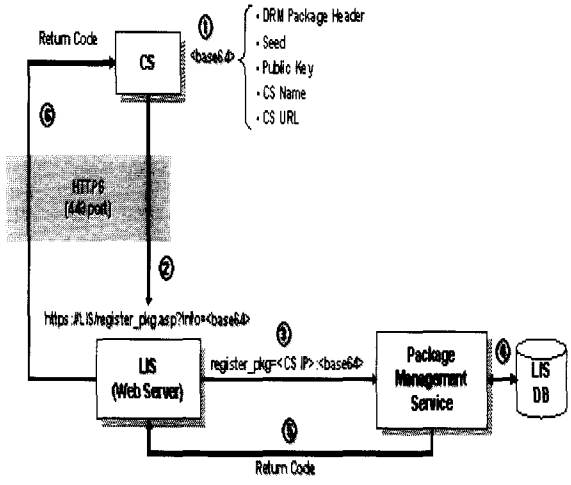
암호화는 서버 측면에서 디지털 인코딩 암호화 과정이고 복호화는 클라이언트 측면에서의 복호화 과정이다

3.2 컨텐츠 암호화의 설계

컨텐츠의 DRM 암호화의 인코딩 작업은 컨텐츠 서버와 라이센스 서버에서 함께 수행되는 구조이다.

3.2.1 컨텐츠 서버의 암호화 설계

컨텐츠 서버에서는 CP(Contents Provider)가 제작한 디지털 컨텐츠가 암호화 도구를 통해서 암호화 컨텐츠가 완성되는 과정으로 (그림 3)과 같은 구조를 가진다.



(그림 3) 컨텐츠 서버에서 암호화 과정

① 컨텐츠 서버는 "DRM Package Header", "Seed", "Public Key", "CS Name", "CS URL"을 Base64 Encoding 하여 <base64>로 구성한다. CS URL은 Client Module이 LIS로 라이센스를 요청할 때 컨텐츠 서버로 재 호출하기 위한 URL이다.

② 컨텐츠 서버는 LIS에 HTTPS 프로토콜로 연결한다. 이때, SSL을 이용하여 LIS에 대한 인증(Authentication) 기능을 수행한다. 이를 위해 LIS는 X.509v3의 보증 기능을 보유하여야 한다. SSL의 Handshake Protocol을 통해 인증을 확인한 후 LIS로 "register_pkg.asp"로 구성한 <base64>를 보낸다.

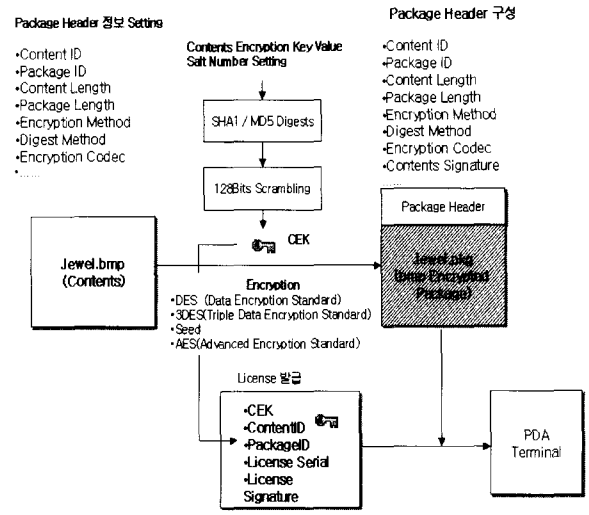
③ register_pkg.asp는 COM 또는 Windows NT Service로 구성된 "Package Management Service"로 "register_pkg = <CS IP> : <base64>" 문자열을 전달한다. <CS IP>는 CS의 IP로써 HTTPS 연결 시 얻어질 수 있다.

④ Package Management Service는 <base64>를 Base64 Decoding한다. "CS Name"과 <CS IP>를 LIS의 DB에 저장되어 있는 값과 비교함으로써 자신이 관리하는 CS인지를 먼저 확인한다. 확인이 이루어지면 LIS에 있는 DB에 이를 등록한다.

⑤ Package Management Service는 해당 DRM Package 등록 처리에 대한 리턴 코드를 생성하여 LIS Web Server의 register_pkg.asp로 넘긴다.

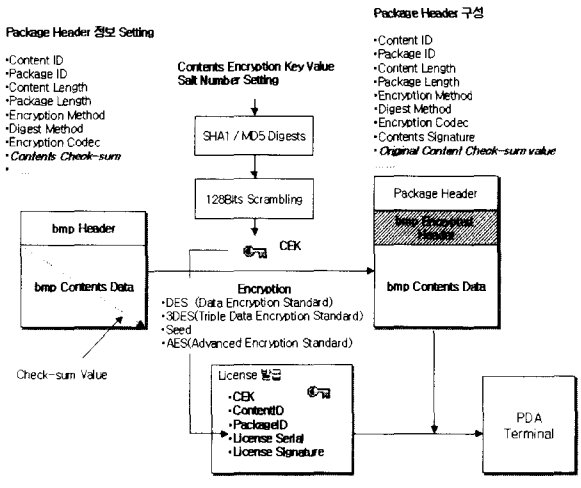
⑥ LIS Web Server의 register_pkg.asp는 컨텐츠 서버에게 리턴 코드를 전달한다.

이와 같은 순서를 통해서 암호화 방법을 적용하였고 일반적인 암호화 방법은 첫째, 전체 암호화로 컨텐츠의 헤더 정보와 컨텐츠 전체를 모두 암호화하는 방법이 있다. 이것은 컨텐츠의 신뢰성 면에서 바람직한 설계 방법이나 컴퓨팅 파워가 부족한 모바일 환경에서는 부 적합한 설계 방법이 될 수도 있다. 예를 들어 운영 체제가 PPC와 Palm을 수용하는 PDA에서 동일한 컨텐츠 복호화 수행 속도가 현저하게 다른 결과가 추출되었다. 그 실험 결과는 차후에 제시하겠다. (그림 4)는 그림 파일에 대해서 전체 암호화 하는 모듈을 제시한 사례이다. 디지털 컨텐츠의 전체 정보와 CEK의 값이 결합되어 Package Header의 구성을 이루며 각각의 정보는 Content ID부터 Contents Signature등을 나타낸다.



(그림 4) 전체 암호화 생성과정

반면에, 부분 암호화는 컨텐츠의 헤더 파일 영역을 위주로 암호화하고 컨텐츠 영역에서 필요 부분만 추출하여 암호화 하는 방법으로 본 시스템에서도 적용한 설계 모듈이다. (그림 4)의 전체 암호화 시스템과 차이점은 헤더 부분과 컨텐츠의 Check-sum Value를 측정하여 Encrypted Header에 반영하는 사항이다. (그림 5)에서 부분 암호화에 대한 설계 모듈을 제시하였다.



(그림 5) 부분 암호화 생성과정

이와 같은 방법등로 패키징된 컨텐츠의 DRM Contents Header Sample을 추출한 결과는 (그림 6)과 같은 형태를 보여준다.

```
00000000h: 01 15 18 63 69 64 3A 41 6C 61 72 6D 31 40 75 61 ; ...cid:Alarm1@ua
00000010h: 6E 67 65 6C 2E 63 6F 6D 61 70 70 6C 69 63 61 74 ; ngel.comapplicat
00000020h: 69 6F 6E 2F 6F 63 74 65 74 2D 73 74 72 65 61 6D ; ion/octet-stream
00000030h: 81 5A EA 30 45 6E 63 72 79 70 74 69 6F 6E 2D 4D ; 걬?Encryption-M
00000040h: 65 74 68 6F 64 3A 41 45 53 31 32 38 43 42 43 3B ; ethod:AES128CBC;
00000050h: 70 61 64 64 69 6E 67 3D 52 46 43 32 36 33 30 3B ; padding=RFC2630;
00000060h: 70 6C 61 69 6E 74 65 78 74 6C 65 6E 3D 31 33 36 ; plaintextlen=136
00000070h: 31 32 0D 0A 52 69 67 68 74 73 2D 49 73 73 75 65 ; 12..Rights-Issue
00000080h: 72 3A 68 74 74 70 3A 2F 2F 77 77 77 2E 64 69 67 ; r:http://www.dig
00000090h: 69 63 61 70 73 2E 63 6F 6D 2F 67 65 74 5F 72 69 ; icaps.com/get_ri
000000a0h: 67 68 74 2E 61 73 70 0D 0A 43 6F 6E 74 65 6E 74 ; ght.asp..Content
000000b0h: 2D 4E 61 6D 65 3A 42 65 6C 6C 5F 52 69 6E 67 5F ; -Name:Bell_Ring_
000000c0h: 77 61 76 0D 0A 43 6F 6E 74 65 6E 74 2D 56 65 6E ; wav..Content-Ven
000000d0h: 64 6F 72 3A 44 69 67 69 63 61 70 73 27 20 42 65 ; dor:Digicaps' Be
000000e0h: 6C 6C 0D 0A 49 63 6F 6E 2D 55 52 49 3A 68 74 74 ; ll..Icon-URI:htt
000000f0h: 70 3A 2F 2F 77 77 77 2E 64 69 67 69 63 61 70 73 ; p://www.digicaps
00000100h: 2E 63 6F 6D 2F 61 6C 61 72 6D 2E 69 63 6F 00 6B ; .com/alarm.ico.k
00000110h: 3E DC 3E 12 BF 38 94 DB 46 EA 65 F8 9E F8 65 A3 ; >?.?붺F???
00000120h: BD B0 65 7B D2 2C 0C 88 F4 0A 9D 38 06 9B 3A 31 ; 쉾e(?.뎧.?.?1
00000130h: 6C 71 F2 E7 BD 16 8E A2 05 6B 86 09 C3 62 A7 DA ; lq陳?렚.k?굊
00000140h: C4 A2 CF 44 C9 F9 0E 7E 81 B4 3C EA C5 30 46 83 ; 칙? .~곣<月0F
00000150h: 22 B9 61 C1 2B 54 C6 1A C3 D6 57 97 83 2B 14 49 ; "뱎?T?쵍W(.I
00000160h: 4F FB 6C 91 22 D4 9F 17 D6 BD A1 A6 F5 03 E9 E2 ; O???.꽆_??
00000170h: C6 9C 52 A1 C6 9D 8D 56 21 2D 95 D0 DC C5 66 65 ; ?R°꼅V!-뼑fe
```

(그림 6) DRM Content Sample Hex View

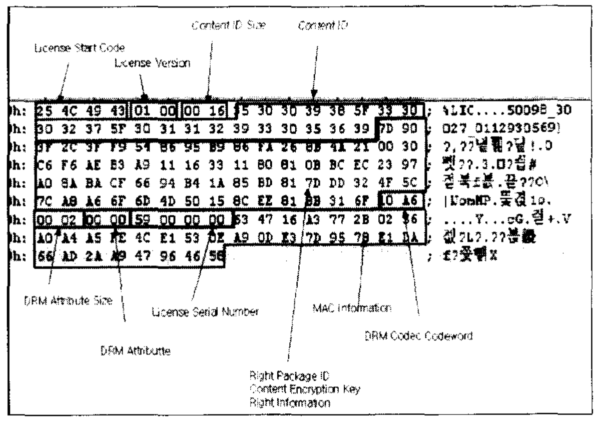
3.2.2 암호화 라이센스 발급의 설계

〈표 2〉 라이센스 키의 정보

Data Type	LicenseInfo : License Information Structure	
Member	Member 설명	타입
szStartCode	License start code	BYTE(4)
SzLicenseVersion	License version	BYTE(2)
sContentIDSize	Content ID size	Uint16
pszContentID	Content ID	BYTE(VAR)
nPackageID	**Packaging ID**	**BYTE(16)**
SpackagingKeySize	**Packaging key Size**	**Uint16**
pszPackagingKey	**Packaging key**	**BYTE(VAR)**
szRightVersion	**Right version**	**BYTE(2)**
sRightSize	**Right size**	**Uint16**
PszRight	**Right information**	**BYTE(VAR)**
sDRMcodeword	DRM codec codeword	Uint16
sAttributeSize	Attributes size	Uint16
pszAttribute	Attributes	BYTE(VAR)
nLicenseSerial	License serial number	Uint16
SzMAC	MAC Information	BYTE(32)

라이센스 서버에서는 새롭게 생성된 DRM 컨텐츠와 매핑되는 라이센스를 생성하고 컨텐츠 사용을 요청하는 PDA에 라이센스를 발급하는 기능을 수행한다. 라이센스 내에 있는 데이터는 크게 해당 DRM Contents의 식별을 위한 정보와, 암호화된 DRM Contents의 CEK, DRM Content 사용의 제한 기능을 갖는 허락(Permission) 및 요청(Constraint) 정보, 그리고, DRM Content의 전자서명(signature) 정보를 포함하고 있다. 이때 라이센스의 형태는 <표 2>와 같다.

<표 2>에서 제시한 라이센스 키의 데이터 타입을 기준으로 (그림 7)과 같은 라이센스 키의 형태가 만들어진다.



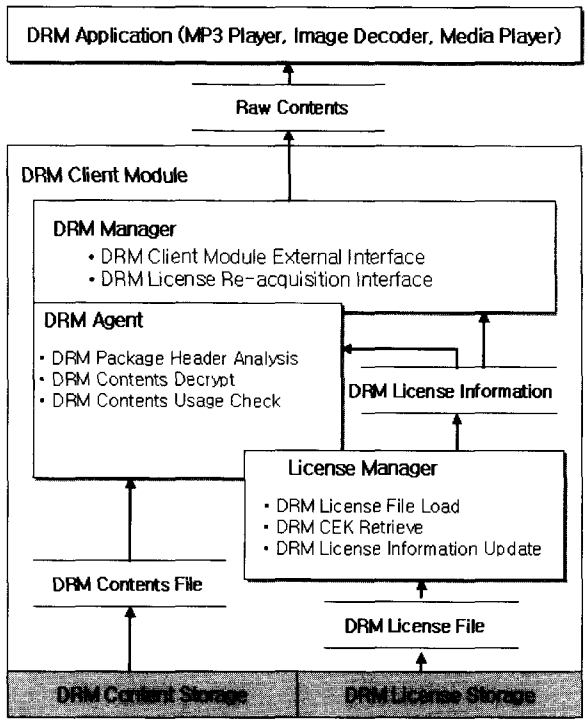
(그림 7) 라이센스키의 구조

(그림 7)에서 라이센스 키는 라이센스 컨텐츠의 헤더 정보와 매핑되는 데이터 즉, Content ID 와 Package ID 정보를 가지고 있다. 컨텐트 유형의 정보, 파일 크기, 컨텐츠 타입 등의 정보를 가지고 있다. 라이센스는 <표 2> 라이센스 구조에서 Package ID, Content Packaging Key, License 내 사용권리, Version 및 Right Constraint Informaton은 공개되지 않아야 하는 중요 정보이므로 이것는 단말 유일의 시리얼(Serial) 및 단말의 전화번호로 서버쪽에서 런타임으로 암호화하여 클라이언트로 전달하게 된다.

3.2.3 디바이스에서의 컨텐츠 복호화 설계

PDA에서는 컨텐츠를 다운 받아 수행할 경우 암호화된 컨텐츠와 동시에 라이센스를 다운로드 받게 된다. 암호화된 DRM 컨텐츠를 Playing, Viewing, Printing 그리고 Executing하기 위한 플레이어 및 어플리케이션은 DRM Client Module로부터 DRM 컨텐츠의 입,출력을 담당하게 된다. DRM Client Module은 Storage로부터 DRM 컨텐츠를 먼저 로드하고 DRM Client Module은 DRM 컨텐츠의 Package Header로부터 해당 DRM 컨텐츠의 라이센스 파일 위치를 확인후 라이센스 파일을 로드한다. 로드된 라이센스 파일로부터 DRM 컨텐츠 활용에 사용 권리 정보를 확인하고 컨텐츠 사용 권리가 없을 경우 암호화된 DRM 컨테츠를 복호화 하지않게 된다. 만약 컨텐츠 사용 권리가 존재할 경우 DRM 컨텐츠을 복호화하여 반환하게 된다. 시스템 대한 일련의 과정을 수행하는 기능이 클라이언트 DRM 모듈의 기능이다.

클라이언트 모듈을 크게 세 개의 영역으로 나누어서 설계하였으며 형태는 (그림 8)과 같다.



(그림 8) 클라이언트 DRM 모듈의 구성

(그림 8)에서는 클라이언트 모듈을 나타낸 사항으로 첫째, DRM Manager는 DRM Application에서 암호화된 컨텐츠의 DRM 패키지를 사용하고자 할 경우에 PDA에 내장된 Player 또는 Viewer에게 DRM Package에 대한 인증 및 접근과 사용에 대한 인터페이스를 제공한다. 또한 DRM 컨텐츠에 대한 License 사용 권리가 만료됐을 경우 License를 재 구매 할 수 있는 URL로 이동하도록 브라우저를 구동하게 하는 기능도 포함한다. 둘째, DRM Agent는 DRM Manager로부터 DRM 컨텐츠 요청 사항을 전달 받아 DRM 패키지에 대한 활용 여부를 확인하고, 암호화된 DRM 컨텐츠를 복호화로 처리한다. DRM 컨텐츠의 활용 여부를 확인하기 위해서 License Manager와 상호 연동된다. 셋째, License Manager는 DRM Package에 대한 라이센스를 관리하는 모듈로 라이센스 파일로부터 CEK를 추출하여 DRM Agent에 전달하며, DRM Agent 또는 DRM Manager의 요청에 따라 보유하고 있는 라이센스 리스트를 조회하고 사용하고자 하는 DRM Package의 License에 대한 사용 횟수, 기간 등 사용 권한의 조회 및 변경 작업을 수행한다. 또한 라이센스 정보는 불법적인 복제 및 변경을 방지하기 위해 레지스트리에 정보를 저장하고 관리하게 된다.

그리고 이전에 제시한 서버측면에서 암호화를 수용할 수 있는 클라이언트 측면에서의 복호화 설계가 필요하다. 그 설계 구조를 함수의 code로 (그림 9)와 같이 설계하였다.

```
전체 복호화 DRM_UnPack()

DWORD DRM_UnPack(char * lpszInp  // INPUT FILE PATH
    PLAYMODE ePlayMode,          // CONTENT PLAY MODE
      UNPACKMODE eUnPackMode,    // UNPACK MODE
      char * lpszMin,            // MIN NUMBER
      char * lpszOutputFile,     // OUPUT FILE PATH
      CONTENTTYPE *pType,        // CONTENT TYPE
      BYTE **ppszOutPutBuff,     // BUFFER POINTER
      UINT *pBytes)              // BUFFER SIZE
```

(a) 전체 복호화를 위한 Function

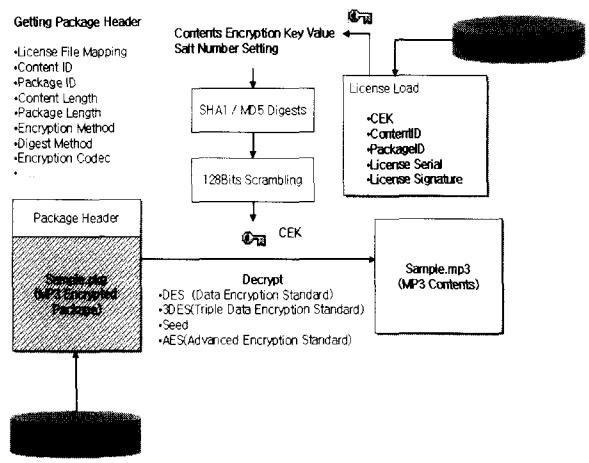
```
부분 복호화 DRM_UnPack()

DWORD DRM_UnPack(APPLICATIONID eAppId
                              // APPLICATION ID
      char * lpszInp          // INPUT FILE PATH
    PLAYMODE ePlayMode,       // CONTENT PLAY MODE
      UNPACKMODE eUnPackMode, // UNPACK MODE
      char * lpszMin,         // MIN NUMBER
      char * lpszOutputFile,  // OUPUT FILE PATH
      CONTENTTYPE *pType,     // CONTENT TYPE
      BYTE **ppszOutPutBuff,  // BUFFER POINTER
      UINT *pBytes)           // BUFFER SIZE
      UINT *nPos)             // RAW BUFFER POSITION
```

(b) 부분 복호화를 위한 Function

(그림 9) 클라이언트에서 복호화 Function 비교

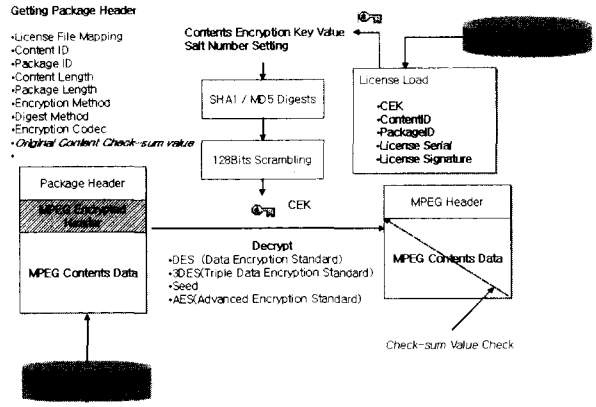
(그림 9)에서 2개의 DRM_UnPack() 함수를 통해 DRM Application으로 원본 컨텐츠를 반환하며 내부적인 암호화된 DRM 컨텐츠의 복호화 과정을 처리하였다. DRM_UnPack()의 파라미터에 인스트럭션의 구분으로 전체 복호화와 부분 복호화의 여부를 결정하여 적용되는 형태로 설계할 수 있다.



(그림 10) 전체 복호화 처리과정

(그림 10)은 전체 암호화되어 있는 DRM 컨텐의 복호화

처리 과정이고, (그림 11)는 부분 암호화되어 있는 DRM 컨텐츠의 복호화 처리 과정이다.



(그림 11) 부분 복호화 처리과정

(그림 11)에서 Package Header에 구성될 Check Sum Value값을 통해서 최소한의 컨텐츠에 대한 무결성을 검증하기 위한 구현 예제로는 (그림 12)와 같다.

```
int checkPacketSum (unsigned char *pack,
                    int packLen)
{
        int i ;
        unsigned char bSum ;
        unsigned char *ptr ;

        ptr = pack ;
        for ( i = 0 ; i < packLen ; i++) {
            bSum += *ptr++ ;
        }
 return bSum ;
}
```

(그림 12) 무결성 검증 예제

4. 프로토타입의 구현 및 분석

본 논문에서 제안한 보안 시스템의 프로토타입 구현을 위한 개발 환경과 실험 결과는 다음과 같다.

4.1 개발 환경

① S/W 구조 : Client/Server 구조
② 모바일 디바이스 : PDA
③ 운영체제 : Palm, PPC
④ 개발언어 : EVC++, Palm Codewarrior
⑤ Crypto 알고리즘 : SEED
⑥ DATA 계열 : 10K~1000K의 이미지 파일
⑦ 측정 대상 : 사이즈별 이미지 파일의 컨텐츠 복호화 Time Tick Countl
⑧ Demension : ms(mili-second)

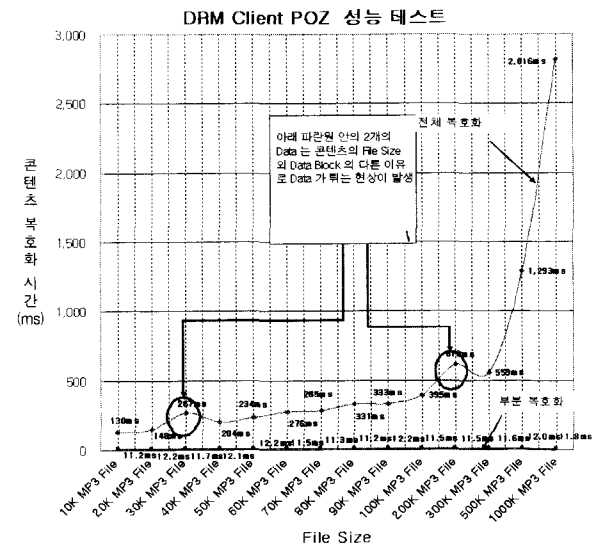
4.2 실험 결과

실험 결과는 PPC를 사용하는 PDA와 Palm을 사용하는 PDA에서 복호화의 수행 속도를 비교하여 제시하였다

첫째, PPC 운영체제를 사용하는 POZ에서의 복호화 수행 속도 시간을 <표 3>과 같이 나타내었다.

〈표 3〉 PPC용 POZ에서의 복호화 실험 결과

Test 단말기	서비스	Algorithm	Test File	Size (Bytes)	Time(ms)	
					전체복호화	부분복호화
POZ	그림친구 서비스	SEED	10K Image	10,909	130	11.2
			20K Image	19,581	148	12.2
			30K Image	30,973	267	11.7
			40K Image	42,877	204	12.1
			50K Image	55,437	234	12.2
			60K Image	64,781	276	11.5
			70K Image	75,661	285	11.3
			80K Image	80,989	331	11.2
			90K Image	95,853	333	12.2
			100K Image	119,534	395	11.5
			200K Image	194,318	613	11.5
			300K Image	299,166	559	11.6
			500K Image	486,334	1293	12.0
			1000K Image	1,089,727	2816	11.8



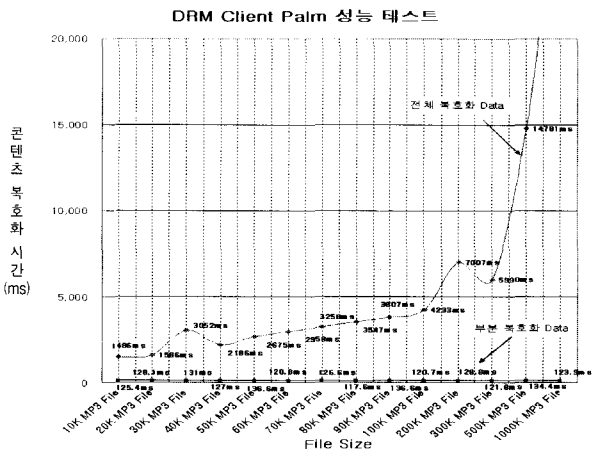
(그림 13) POZ 단말기에서 복호화 수행속도 그래프

(그림 13)같이 PPC용 PDA에서도 복호화 수행 속도는 암호화된 컨텐츠의 블록 사이즈에 비례하는 결과를 보여주고있다. 따라서 전체 암호화된 컨텐츠를 복호화 처리하는 것보다는 헤더만 부분 복호화 처리할 경우 현저한 속도 개선을 보여주고 있다.

둘째, Palm 운영 체제를 사용하는 M330에서 복호화 처리속도를 비교한 실험 결과를 <표 4>에서와 같이 나타내었다.

〈표 4〉 Palm용 M330의 복호화 실험 결과

Test 단말기	서비스	Algorithm	Test File	Size (Bytes)	Time(ms)	
					전체복호화	부분복호화
Palm M330	그림친구 서 비 스	SEED	10K Image	10,909	1486	125.4
			20K Image	19,581	1586	128.1
			30K Image	30,973	3052	131.0
			40K Image	42,877	2186	127.0
			50K Image	55,437	2675	136.6
			60K Image	64,781	2958	120.8
			70K Image	75,661	3258	126.6
			80K Image	80,989	3547	117.6
			90K Image	95,853	3807	136.6
			100K Image	119,534	4233	120.7
			200K Image	194,318	7007	128.8
			300K Image	299,166	5990	121.8
			500K Image	486,334	14781	134.4
			1000K Image	1,089,727	30179	123.9



(그림 14) M330 단말기에서 복호화 수행속도 그래프

Palm 운영체제를 사용하고 있는 M330 MITs 단말기는 xScale을 사용하고 있는 PPC 계열의 POZ 단말기보다도 뚜렷한 성능저하 현상을 보여주고 있다. 그러나 일정한 크기의 컨텐츠 Header만을 복호화 처리할 경우 125ms 안팎의 Time Tick Count의 처리 결과를 얻는 것을 확인할 수 있었다.

결론적으로 모바일 환경에 적합한 형태의 암호화 설계는 현재의 컨텐츠 특성과 파일 크기, 그리고 단말기 수행 능력이 고려된 상태에서 설계되어야 한다는 것을 알 수가 있다.

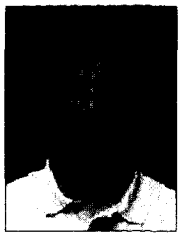
5. 결 론

본 논문에서는 무선 인터넷에서 유통되고 있는 디지털 컨텐츠의 저작권을 보호하기 위하여 모바일 보안 시스템의 설계를 제안하였다. 특히 컨텐츠 암호화 과정에서 전체 암호화와 부분 암호화의 적용 결과를 비교하여 보았다. 그 결과 무선 환경에서는 디바이스의 처리 능력을 고려하여 암호화 설계가 이루어지는 것이 중요하다는 사항을 다시 한번 검증하게 되었다. 모바일 디지털 저작관리시스템은 국내에서 아직 초기 단계에 있으며 연구 자체도 미약하다. 일반 유선 웹에서의 DRM은 이미 개발되어 상용화되고 있는 반면에 모바일 분야에서 미약한 이유는 무선 환경의 통신 속도의 문제와 디바이스 처리능력이 제한적이라는 사항이다. 기술의 개발에 따라서 이러한 문제는 차후에 해결 되겠으나, 모바일의 경량화 특성상 클라이언트의 메모리 용량을 고려하여 수행되는 구조의 DRM 설계 방법이 적용되어야 할 것이다.

향후의 연구 계획은 본 논문에서 제안한 DRM 설계 방법을 고도화하고 처리 능력이 제한적인 디바이스에서도 원활한 수행이 가능한 복호화 가속기를 개발하고자 한다. 이 개발 방법론을 PDA뿐 아니라 전체의 임베디드 시스템에 적용될 수 있는 구조로 확대하여 연구할 계획이다.

참 고 문 헌

[1] Extensible Rule Markup Language Version 2.0, http://www.xrml.org, 2002.
[2] F. Hartung, F. Ramme, "Digital rights management and watermarking of multimedia content for m-commerce applications," IEEE Communications Magazine, Vol.38, No.11, pp. 78-84, 2000.
[3] Joshua, D. Susan, K., "Understanding DRM System," An IDC White Paper, IDC, 2001.
[4] L. J. Camp, "First Principle of Copyright for DRM design," IEEE Internet Computing, Vol.07, No.03, pp.59-65, 2003.
[5] Mobile DRM http://www.nds.com/mobile_solutions/mobile_drm_solutions.html.
[6] MPEG-21 Part 4 : MPEG-21 Intellectual Property Management and Protection(IPMP) Version 5, Moving Picture Experts Group, 2002.
[7] OMA Digital Rights Management Version 1.0, Open Mobile Alliances, 2002.
[8] R. G. van Schyndel, A. Z. Tirkel, N. R. A. Mee, C. F. Osborne, "A digital watermark," IEEE International Conference on Image Processing, Austin, Texas, USA, Vol.2, pp.86-90, 1994.
[9] 권순홍, "실시간 멀티미디어 서비스의 DRM 적용방법 설계", 정보과학회 춘계학술대회, Vol.29, No.1, pp.481-483, 2002.
[10] 김정현, 윤기송, 박창순, "MPEG-21 IPMP를 고려한 DRM 기반 유통시스템 구현", 정보처리학회 추계학술대회, Vol.9, No.2, 2002.
[11] 박봉련, 김태윤, "디지털 저작권 관리에서 사용자의 프라이버시 보호를 제공하는 라이센스 관리 프로토콜", 한국정보과학회논문지B, Vol.30, No.2, pp.189-198, 2003.
[12] 박주상, 윤기송, 박창순, "Microsoft의 디지털 저작권 보호 기술 분석 및 향후 시스템 개발 요소", 정보처리학회 추계학술대회, Vol.9, No.2, 2002.
[13] 윤감규 역자, 전자보안시스템, 동일출판사, 1996.
[14] 이용호, 이임영, "공개키 기반 구조에서의 키 복구 지원 메커니즘", 한국정보처과학회 춘계학술대회, Vol.29, No.1, pp.766-768, 2002.
[15] 장우영, 신용탁, 신동일, 신동규, "DRM시스템에서 Publisher 시스템의 설계", 한국정보과학회 추계학술대회, Vol.28, No.2, pp.544-546, 2001.
[16] 정재권, 류대길, 강한 공역, 보안과 암호화, 인포북, 2001.
[17] 한국 디지털 콘텐츠 포럼, 디지털 유통 프레임 워크 구축 및 기술표준 전략 수립에 관한 연구, 2002.



김 후 종

e-mail : hjkim2@sktelecom.com

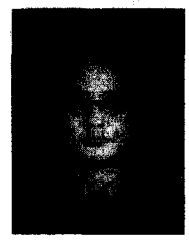
1988년 서강대학교 전자공학과(학사)

1995년 서강대학교 전자공학과(석사)

2000년~현재 국민대학교 대학원 전자공학과 박사과정 수료

1994년~현재 SK텔레콤 Platform 연구원 Terminal 개발팀장 근무중

관심분야 : 모바일 컴퓨팅, 모바일 보안, RF



나 승 원

e-mail : nasw@sktelecom.com

1993년 단국대학교 농경제학과(학사)

1996년 단국대학교 전자정보관리(석사)

1999년~현재 동국대학교 대학원 컴퓨터공학과 박사과정 수료

1997년~현재 SK텔레콤 Platform 연구원 Terminal 개발팀 과장 근무중

관심분야 : 모바일 프로그래밍, 이동 에이전트, 모바일 보안