韓國 컴퓨터情報學會 論文誌
第11卷 第2號, 2006. 5.

2006-11-2-2-8

프로그램 온라인 등록 시스템기반의 저작권 보호시스템 설계 및 구현

장 재 혁*, 이 종 섭**, 최 용 락***

Design and Implementation of a Copyright Protection System base on the Program on-line Registration System

Jang Jae Hyeok*, Lee Jong Sup**, Choi Yong Rak***

요 약

프로그램 저작물의 지적재산권 보호를 위해 저작자는 프로그램 심의조정위원회에 등록하여 저작권을 보호 받는다. 프로그램 등록은 off-line과 on-line으로 처리되고, on-line을 통한 프로그램 등록은 프로그램 등록자의 편의성 제공과 함께 저작물을 외부의 저작권 침해요소로부터 보호한다. 그러나, 등록된 저작물의 무결성과 기밀성은 내부의 위험요소(시스템 오류, 내부 관리자 불법접근 및 수정)에 보장 받지 못하는 단점이 있다. 본 논문에서는 저작물 기밀성, 무결성 보증과 다중서명메커니즘을 이용하여 내부의 시스템 오류 및 내부자에 의한 저작물 침해요소로부터 신뢰된 저작물을 보장하고, 전자서명 관리의 편의성을 제공하는 시스템을 제안한다.

Abstract

Writers enroll their outcome to Program Deliberation & Mediation Committee and get the copyright preserved for the protection of IPR. The program registration is conducted through off-line and on-line methods, and especially on-line registration provides program registrants convenience along with the safety of property from external copyright invaders. However, it is a shortcoming that the integrity and confidentiality of the enrolled program cannot be guaranteed in case of internal factors such as system errors, administrator's illegal access and revision. This paper proposes the reliable system, ensuring programs and offering convenience of Digital signature management from the system errors and intruding factors by internal administrator, using the security of confidentiality, integrity and Multi-Signature Scheme for program.

▸ Keyword : Copyright(저작권), IPR(지적재산권), Authentication(인증), Integrity(무결성), Digital Signature(전자서명)

• 제1저자 : 장재혁
• 접수일 : 2006.03.31, 심사완료일 : 2006.05.24
* 대전대학교 컴퓨터공학과 박사과정, ** 한국군사문제연구원 정보통신시스템 IT담당 부장
*** 대전대학교 컴퓨터공학과 정교수

Ⅰ. 서 론

국내에서는 컴퓨터 프로그램 저작권 보호를 위해 프로그램심의조정위원회(PDMC: Program Deliberation & Mediation Committee)를 설립하여 저작자가 개발한 프로그램을 등록함으로써 프로그램의 창작사실을 명확히 하며, 창작연월일을 추정함으로써 저작권자의 권리보호와 거래의 안전을 도모할 수 있도록 적극적인 보호활동을 하고 있다. 그 결과 현재 컴퓨터프로그램 등록건수는 10만건 이상으로 매년 꾸준한 증가세를 보이고 있는 실정이다.

프로그램 등록업무란 저작자가 개발한 프로그램을 봉인하여 PDMC 내에 보관하고 신청서에 기재된 프로그램등록에 대한 내용을 데이터베이스에 보관함으로써 등록된 내용을 프로그램 공보와 인터넷 및 PC통신망 등을 통하여 등록정보를 공개하여 중복투자 방지 및 공정한 이용 촉진을 도모한다[1,2,3].

off-line상에서의 프로그램등록은 각 지역 현장사무소 부재로 인하여 지역간의 불편을 호소하는 민원제기가 발생하고, 등록 프로그램 정보의 제공으로 중복투자 및 개발방지에 대한 욕구가 증대되고 있다. 이런 문제는 프로그램 온라인 등록시스템을 개발하여 운영함으로서 해결되었다.

프로그램 저작물은 불법수정 및 도용, 파손, 네트워크를 통한 저작물 침해 등의 위험요소가 발생한다. 또한, 저작권 침해가 발생하여 저작권 법적공방시 등록된 저작물이 파손 및 변경되었는지 저작자 입장에서는 신뢰할 수 없는 환경을 제공한다. 저작물의 침해가 발생한다는 것은 디지털콘텐츠 시장을 위축시키는 요인으로 작용한다[4]. 등록된 저작물의 신뢰성 보장을 위해 본 논문에서는 저작물의 신뢰된 제 3의 시스템을 운영함으로서 신뢰성을 보장 받는 저작물을 제공하고자 한다.

Ⅱ. 프로그램 등록시스템 분석

2.1 시스템 보안 요구기능

디지털영역에서 저작물은 불법 수정 및 도용, 파손, 네트워크를 통한 저작물 침해 등의 위험요소가 발생한다. 이러한 위험요소로부터 저작물을 보호하기 위해 안전한 저작물의 관리가 필요하다[5].

프로그램 저작물과 저작자 보호를 위한 관리시스템의 요구사항은 다음과 같다.

가. 저작물 저작권 보호: 창작된 저작물 등록을 통하여 저작자의 저작권을 보호

나. 저작물 무결성 검증: 저작물이 원본과 동일한 형태로 관리되어 추후 저작권 침해가 발생하였을 경우 대조될 수 있도록 저작물을 관리

다. 저작물의 기밀성: 저작물은 인가되지 않은자로부터 보호

라. 저작자와 프로그램 등록 시스템간의 상호 인증: 저작자와 프로그램 등록시스템간의 쌍방 인증을 통한 저작물 등록 및 관리

마. 저작물 보호 정책: 저작물 보호를 위한 접근 권한 및 정책을 수립하여 외부의 위험요소로부터 저작물 보호 정책을 수립

바. 저작물 관리 정책: 원본의 저작물이 변형된 형태가 아님을 검증하고 추후 저작물 침해의 문제 및 보관에 필요한 관리 정책 수립

저작물 보호를 위한 관리 시스템은 디지털 콘텐츠 시장에서 문제되는 불법복제 및 유통으로부터 저작자의 권리를 보호하고 빠르고 쉬운 프로그램 등록 환경을 제공하여 콘텐츠 시장의 활성화를 유도하는 시스템이다. 즉, 저작자의 저작권을 보호하여 안전한 디지털콘텐츠 시장을 구축하는데 목적이 있다.

2.2 프로그램 등록시스템 구성

프로그램 온라인 등록시스템은 사용자영역의 등록 에이전트와 인증기관, 프로그램 등록시스템, 금융결제원의 4개 영역으로 구성된다. 각 개체의 기능은 다음과 같다.

- 등록 에이전트: 저작물을 등록하는데 필요한 클라이언트
- 인증기관: 사용자 인증을 위한 인증서 관리기관
- 프로그램 등록시스템: on-line 상에서 프로그램 등록업무를 총괄관리
- 금융결제원: 프로그램 등록에 필요한 수수료 결제관리

프로그램 등록시스템 구성요소들은 Fig. 1과 같이 개체간 인터페이스에 의해 업무가 처리된다[1,2,3].

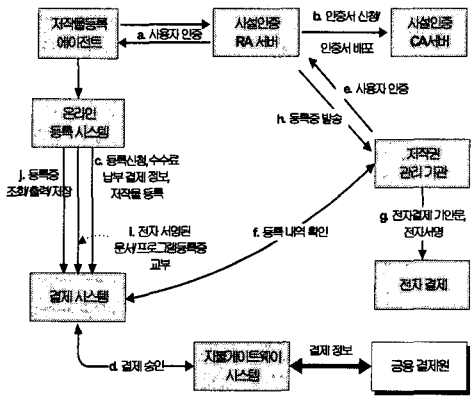

그림 1 프로그램 등록 시스템 등록
Fig. 1 Construction of a program registration

a. 사용자 인증: 사용자 등록에 의해 인증서를 발급 받아 인증서 로그인
b. 인증서 신청 발급 및 배포: 사용자로부터 요청된 인증서 발급 신청은 인증관리 서버로부터 신분 확인 후 발급
c. 등록신청(등록 신청정보 암호화 + 인증서에 의해 인증되어진 전자서명), 수수료 납부 결제 정보, 저작물 등록: 등록 신청정보의 암호화와 인증서에 의해 인증되어진 전자서명, 저작물을 수수료 결제 확인 후 등록
d. 결제승인: 신용카드 및 무통장 입금에 의해 결제승인
e. 사용자 인증: 배포된 인증서에 의해 사용자 인증
f. 등록내용 확인: 사용자 및 저작물 등록정보 확인 요청
g. 전자결재/기안문/전자서명: 결제 정보, 기안문, 인증된 전자서명 확인
h. 등록증 발송: 사용자로부터 등록 신청된 저작물에 대한 등록증을 발송
i. 전자 서명된 문서와 프로그램 등록증 교부: 프로그램 등록 및 관리에 필요한 정보 확인 및 요청
j. 등록증 조회와 출력, 저장: 등록된 정보 관리

프로그램 등록은 사용자 인증을 요구한다. 인증된 사용자는 온라인을 통한 등록 신청서 양식에 따른 작성과 등록에 필요한 수수료를 결제하여 저작물을 등록할 수 있다. 웹 서버에서 제공하는 저작물 보호 정책과 기능에 의해 저작물은 네트워크를 통해 보호되어 저작물 관리 시스템에 등록되어 관리된다. 이렇게 등록된 저작물은 추후 저작물의 법적 분쟁시, 근거자료로 활용된다.

프로그램 등록시스템은 온라인 등록시스템, 사용자 영역의 저작물 등록에이전트, 저작물 관리시스템, 상호 보안 인터페이스 영역으로 구분하여 분석한다.

(1) 온라인 등록 시스템

온라인 등록을 통한 저작물 등록은 저작물 등록자와 프로그램 등록시스템의 메인 관리서버의 상호 인증으로 처리된다. Fig. 2는 온라인 등록관리 모듈 구성을 나타낸다.

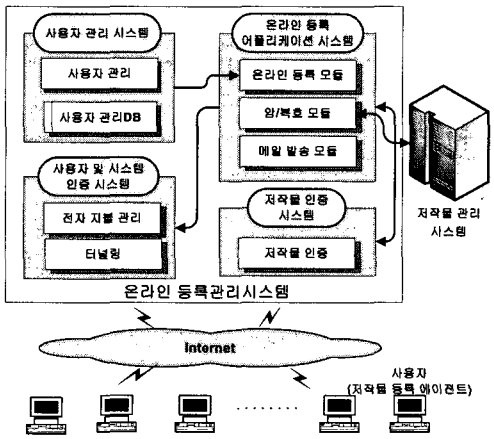

그림 2 온라인 등록 관리 모듈 구성
Fig. 2 Construction of a on-line registration management module

온라인 등록 시스템은 사용자 관리 시스템, 온라인 등록 어플리케이션 시스템, 사용자 및 시스템 인증 시스템, 저작물 인증 시스템으로 구성되고 등록된 저작물 보호를 위한 저작물 관리 시스템과 사용자 영역의 저작물 등록 에이전트에 의해 저작물 등록이 이루어진다.

- 사용자 관리 시스템: 사용자 관리를 위한 시스템
- 온라인 등록 애플리케이션 시스템: 온라인을 통해 등록된 저작물 등록을 위한 기능, 저작물 보호를 위한 암/복호화 기능, 등록 시스템과 사용자간의 정보를 주고받기 위한 전자우편 관리 기능을 제공
- 사용자 및 시스템 인증 서버: 안전한 저작물 보호를 위한 저작물 등록자 및 저작자 인증 서비스와 등록 시스템과의 상호 인증 기능을 제공하고 키 관리 및 분배 기능을 제공
- 저작물 인증 시스템: 등록된 저작물의 저작권 인증 기능 제공

(2) 저작물 등록 에이전트

사용자 영역의 저작물 등록 에이전트는 저작물을 안전하게 전송 관리를 위해 Fig. 3과 같은 기능을 제공한다. Fig. 3은 사용자 영역의 저작물 등록 에이전트를 나타낸다.

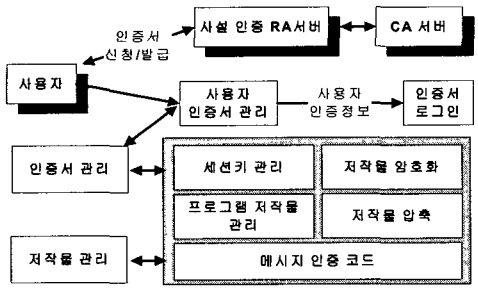

그림 3 저작물 등록 에이전트
Fig. 3 Agent for a copyright registration

사용자 영역의 에이전트는 세션키 관리, 프로그램 저작물 관리, 저작물 압축 및 암호화 기능으로 구성된다. 또한 데이터 관리로서 인증서 관리, 저작물 관리 데이터베이스로 이루어진다. 에이전트 기능은 다음과 같다.

- 세션키 관리: 저작물을 암호화 하는데 사용되는 키로써 프로그램 등록 서버와 상호 인터페이스에 의해 형성된 키이다. 저작물의 기밀성 기능을 지원
- 프로그램 저작물 관리: 저작자가 등록하고자하는 저작물을 관리
- 저작물 암호화: 인가되지 않은 제 3 자로부터 저작물의 기밀성 기능을 제공
- 저작물 압축: 여러 파일로 구성된 프로그램 관리, 저작물 관리 및 전송의 유용성 제공

사용자는 사설 인증 RA(Registration Authority)로부터 사용자 인증서를 신청하고, 프로그램 관리 서버와 안전한 통신을 위하여 인증 서비스를 제공 받는다. 인증서 신청 요청에 의해 RA는 인증서를 배포하고 배포된 인증서를 기반으로 시스템 로그온시 사용자 인증이 이루어진다[6,7].

온라인 등록 시스템은 저작물 보호를 위해 압축 및 암호 서비스를 제공한다. 시스템간의 상호인증에 의하여 설정된 세션키를 기반으로 키 관리 및 분배가 되고, 프로그램 등록 시스템에서 저작물 보호에 이용되는 키로 사용된다. 압축 및 암호화된 저작물은 프로그램 관리 서버에 전송된다. 압축과 암호화는 네트워크 트래픽의 효율과 네트워크 환경에서의 기밀성 서비스를 제공한다.

(3) 저작물 등록 보안 인터페이스

사용자 영역의 에이전트는 저작물 등록 관리시스템과 연계되어 보안채널을 설정한다. 보안설정은 SSL Turni -ng을 기반으로 이루어진다. Figure 4는 저작물 등록을 위한 사용자 영역의 에이전트와 등록 서버의 상호 보안 인터페이스를 나타낸다.

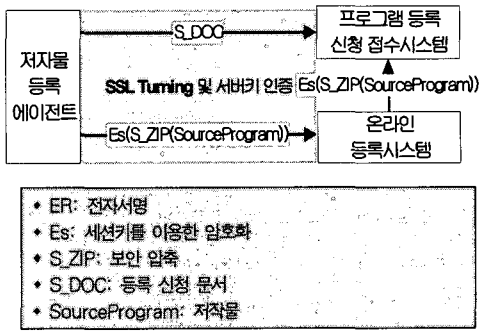

그림 4 프로그램 등록 보안 인터페이스
Fig. 4 Security interface for a program registration

등록 신청서는 개인키를 이용하여 전자서명 하고, 전자 서명된 저작물은 프로그램 등록 접수시스템에 전송된다. 저작물은 보안 압축이 이루어진다. 즉, S_ZIP(Source -Program)은 3중DES에 의해 암호화되어 온라인 등록 시스템에 전송되고 전자결재 확인 후 저작물을 등록한다[7,8,9,10].

(4) 저작물 관리시스템

저작물 관리시스템은 세션키로 암호화된 소스 프로그램을 저작물 관리 데이터베이스에 저장하고 사용자별 저작물 암호화에 사용된 세션키를 사용자관리 데이터베이스에서 관리한다. Fig. 5와 같다.

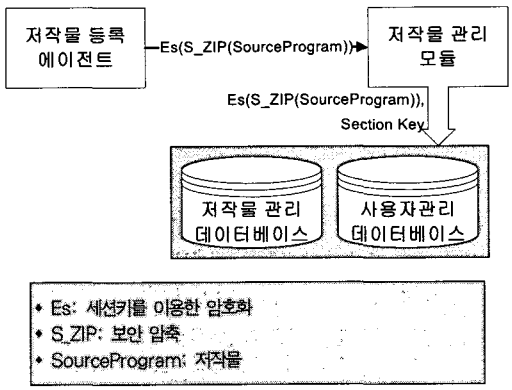

그림 5 저작물 관리 시스템
Fig. 5 Copyright management system

저작물 관리 데이터베이스는 Es(S_ZIP(SourceProgra -m)), 사용자 정보, 등록정보, 전자서명 값을 포함한다. 또한 사용자 관리 데이터베이스는 사용자별로 저작물 등록 리스트, 사용자 기본 신상정보, 개인식별 코드, 저작물별 세션키 등을 포함한다.

2.3 저작물 등록시스템의 보안 위험성 및 효율성 분석

저작물 등록시스템은 시스템 보안 요구기능에서 저작물 무결성, 저작물 기밀성, 저작물 보호정책에 취약성을 가진다. 또한, 공동저작자가 20명 초과시 온라인으로 등록이 가능하지 않다는 문제점을 갖는다.

첫째, 저작물 무결성, 저작물 기밀성, 저작물 보호정책의 취약성은 등록된 저작물의 위변조와 저작물 접근제어에 문제가 있다. 등록된 저작물은 저작물 관리시스템에서 관리된다. 추후, 저작권 침해문제의 법적 공방시 저작물 관리데이터베이스에 저장된 저작물을 이용하여 저작자의 저작권을 인증 받을 수 있다. 그러나 저작물은 세션키에 의해 암호화된 저작물과 세션키를 프로그램 등록시스템의 저작물/사용자 관리 데이터베이스에 보관하고 관리한다. 즉, 등록된 저작물은 파손 및 변경의 위험성을 갖는다. 저작물 저작자의 동의 없이 저작물이 변경될 수 있다는 저작권 침해의 요인으로 작용할 수 환경을 갖는다.

둘째, 공동저작자 초과 문제이다. 공동 저작자가 20명이 초과 될 때는 온라인으로 프로그램을 등록할 수 없는 환경을 갖는다. 즉, off-line으로 직접 방문하여 프로그램을 등록해야한다. 프로그램 저작물은 프로그램 등록자가 온라인을 통해 프로그램 등록을 한다. 공동저작자의 경우, 공동저작자로 포함된 모든 저작자는 프로그램 등록에 동의하는 "위임"을 해야 한다. 위임시 모든 공동 저작자는 전자서명을 한다[11]. 공동저작자가 N명인 경우, N * (단일서명)의 공간이 필요하다. 이런 방식은 저장 공간과 서명 관리에 비효율성을 제공한다.

이러한 문제점을 해결하기 위해 본 논문에서는 저작물의 기밀성과 무결성 서비스를 제공하고 20명으로 한정된 전자서명 기능을 보완한 시스템을 제안한다.

III. 제안 시스템 설계

제안 시스템은 프로그램 온라인 등록 시스템 환경에서 저작물의 안전한 관리 기능을 제공하기 위해 저작물 관리시스템을 제안한다.

3.1 프로그램 저작물 보호시스템

(1) 시스템 구성

저작물 관리시스템과 백업 관리시스템으로 구성된다. 저작물 관리시스템은 프로그램 등록 에이전트로부터 전송된 프로그램 저작물과 저작자 정보를 저작물/사용자 관리 데이터베이스에 저장하고 백업 관리시스템으로 전송하여 안전하게 저작물을 보호한다. 백업 관리시스템은 신뢰된 제 3의 시스템 영역이다. Figure 6은 프로그램 저작물 보호를 위한 시스템 구성이다.

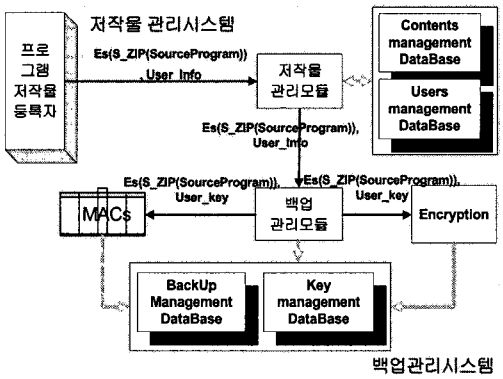

그림 6 프로그램 저작물 보호시스템 구성도
Fig. 6 System construction for program copyright protection

(2) 저작물 관리시스템

저작물 관리시스템은 프로그램 등록에 직접적 운영에 필요한 시스템으로서 저작물 등록에 필요한 프로그램 저작물과 저작자에 대한 관리 기능을 제공한다. 프로그램 저작자의 저작물 보호를 위해 저작물 관리시스템은 Fig. 6과 같이 처리되며 절차는 다음과 같이 처리된다.

단계 1, 프로그램 등록자로부터 저작물 등록에 필요한 정보(User_Info:등록자/저작자 정보, Es(S_ZIP(SourcePr-ogram)): 세션키로 암호화된 저작물)를 저작물 관리시스템에 전송한다. 단계 2, 저작물 관리 모듈은 저작물 관리번호를 부여한다. 단계 3, 사용자/콘텐츠 관리데이터베이스에 저작물과 고유 관리번호를 사용자 정보와 연계하여 저장한다. 단계 4, 저작물 암호화에 사용된 세션키, 암호화된 저작물, 사용자 고유 ID, 저작물 관리번호를 백업관리시스템에 전송한다.

(3) 백업 관리시스템

저작물과 저작권 보호를 위한 신뢰된 제 3의 시스템영역이다. 정상적으로 등록된 저작물은 저작물 관리시스템에서 발생할 수 있는 해킹 및 시스템 오류 등 정보의 무결성 기능을 제공하고 처리되는 절차는 다음과 같다.

단계 1, 저작물 관리시스템으로부터 전송된 정보(저작물 암호화에 사용된 세션키, 암호화된 저작물, 사용자 고유 ID, 저작물 관리번호)를 수신한다. 단계 2, 보안 인터페이스에 의해 형성된 채널을 이용하여 등록자 고유 비밀키를 수신한다. 단계 3, 저작물에 비밀키를 이용하여 암호화 알고리즘 SEED을 적용한 MACs 값을 생성한다. 단계 4, 저작물에 비밀키를 이용하여 SEED 알고리즘을 적용한다. 단계 5, MACs 생성값과 저작물에 SEED 적용값을 백업 관리 데이터베이스에 저장한다. 단계 6, 보안 채널 설정과 저작물 암호화에 사용된 키 값을 키관리 데이터베이스에 저장한다.

백업 관리데이터베이스는 저작권의 생성과 변경시에 기본적으로 추가만 가능하도록 제공한다. 즉, 저작권 이전으로 발생하는 저작권 변경의 경우, 기존의 저작권 고유관리 번호를 인덱스로하여 변경된 저작권 정보를 생성한다.

3.2 프로그램 저작권 인증시스템

(1) 인증 정책 구조

프로그램 저작물은 단일 저작자와 공동 저작자에 의한 등록의 두 가지 영역으로 구분되어 저작물을 등록할 수 있다. 저작물 전자서명의 경우, 저작자로 포함된 모든 저작자의 전자서명 필요하다.

프로그램 저작권을 보호하기 위한 기법으로 저작자의 전자서명을 받는다. 전자서명은 단일인 경우에는 한번의 전자 서명이 이루어지고 공동저작자의 경우는 모든 저작자가 전자서명을 한다. 단일 전자서명은 저작자 본인의 전자서명이 한번 이루어지고, 공동 저작물은 〔저작자(1), 저작자(2), ……, 저작자(N)〕로부터 모든 전자서명을 받는다. 공동 저작자의 전자서명의 우선순위는 고려되지 않으나, 전자서명 인증을 위한 복호에 필요함으로서 전자서명 순서 리스트는 저장/관리한다.

(2) 인증 알고리즘

저작권 인증을 위한 전자 서명은 식(3.1)과 같다.

서명자 U1, U2, U3,……, Un에 대한 전자서명

$$M(Sn) = (S_{KRun}(S_{KRu2}(S_{KRu1}(Copyright)))) \cdots\cdots\cdots (3.1)$$

저작물의 저작자 수에 따라 전자서명은 이루어진다. 공동저작물은 식(3.1)에서와 같이 N번의 전자서명이 필요하다. 공동저작자의 경우, 저작권(Copyright)에 대해서 U1의 개인키로 전자서명 ($S_{KRu1}(Copyright)$)), U2의 개인키로 전자서명 ($S_{KRu2}(S_{KRu1}(Copyright))$)전자서명되고 저작자 N명에 대해 ($S_{KRun}(\cdots(S_{KRu2}(S_{KRu1}(Copyright))))$)로 다중 전자서명이 이루어진다. 식(3.1)을 확장하여 N명의 전자서명 알고리즘은 Fig. 7과 같다.

```
for i = 1 to n { :: n번의 서명
   m' = R(m)
   S = m'^d (mod Uin)
   m' = Suie (mod uin) :: (Uin, Uie)은 User i의 공개키
   if (m'∈MR)
   then
        m = R^-1(m') ;
   else
        exit();
}
```

- i = n번의 서명중의 i 번째 서명자
- $m' = R(m)$, $S = m'^{d} \pmod{U_{in}}$: 개인키를 이용한 서명
- $m' = Su_{ie} \pmod{u_{in}}$: 공개키를 이용한 서명 검증

그림 7 다중서명 알고리즘
Fig. 7 Multi-signature algorism

다중서명 알고리즘은 각 서명의 생성 값이 정확한지를 확인하기 위한 검증 기능을 제공한다. 다중서명의 경우 일부가 손상되었을 경우 다수의 서명에 영향을 미칠 수 있으므로 각 스텝별 서명 검증을 통한 메시지 인증 서비스를 제공한다.

IV. 제안시스템 분석 및 평가

4.1 제안시스템 실험

제안시스템 Sun E220R(온라인등록, 저작물/저작권 관리, 저작물/저작권 백업시스템), Oracle 9i(저작물 관리데이터베이스), IBM LT 03840[Tape](백업 관리데이터베이스) 환경에서 실행된다. 또한 개발 환경은 웹 등록(Java, JSP, HTML), 클라이언트와 서버 인터페이스 포맷(XML), 네트워크 인터페이스(Pro C), 압축 및 암호화(Pro C)를 이용하였다.

(1) 보안 채널 설정

실행 화면은 프로그램 등록시스템에 저작물 관리와 저작권 인증 시스템이 탑재되어 운영되는 과정을 보인다. 사용자 영역에서 프로그램 등록관리 웹 서버에 접속하면 사용자 PC와 서버간의 보안 채널을 설정한다. 보안 채널 설정 화면은 Fig. 8과 같다.

보안 채널은 사용자 영역의 클라이언트와 프로그램 등록 관리 시스템간의 외부로부터 정보보호 기능을 제공한다. 사용자 시스템과 등록 시스템간의 상호 보안 채널 설정 후 서비스가 이루어진다.

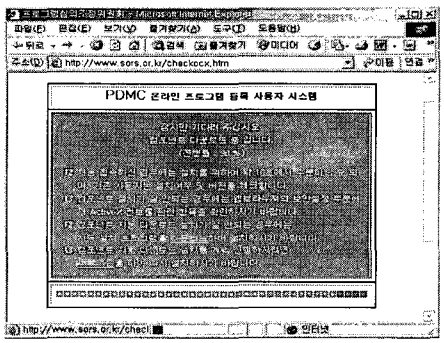

그림 8 클라이언트와 서버간의 보안채널 설정 화면
Fig. 8 Setting of security channel between client and server

(2) 저작물 및 저작권 암호화

프로그램 저작물 등록시, 저작권은 Fig. 9와 같이 암호화 되어 전송된다. 적용된 암호화 알고리즘은 SEED이고 키는 세션키를 활용한다. 세션키는 보안 채널 설정에 생성된 키 값이다.

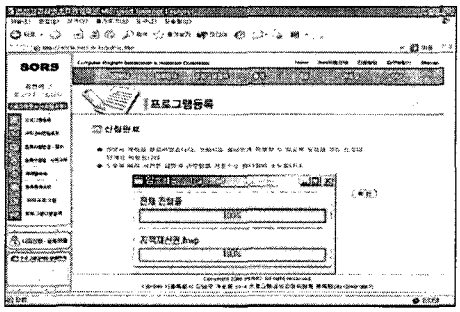

그림 9 저작물 암호화 진행 화면
Fig. 9 Progress status of copyright encryption

프로그램 등록 신청에 의해 신청서가 작성되고 저작물이 압축과 암호화되어 서버의 저작물 관리 데이터베이스에 저장된다. 이로써 사용자와 서버간에 프로그램 등록을 위한 응용 프로그램은 완료된다.

4.2 성능 분석

기존 시스템의 문제는 프로그램 저작물 등록 시스템에서 저작물의 위변조와 접근제어 문제로 발생하는 저작물의 무결성/기밀성, 저작물 보호 정책의 취약성과 온라인을 통한 프로그램 저작물 등록시 공동저작자의 전자서명 기술에 의한 저장 공간 및 서명 관리의 비효율성에 있다.

(1) 프로그램 저작물 보호

등록 시스템내에서 발생할 수 있는 보안 서비스의 취약점은 저작물 관리시스템 이외에 제 3의 신뢰시스템인 백업 관리시스템에 의해 보완된다. 기존 시스템은 저작자와 프로그램 등록 시스템간에 공유된 세션키를 이용하여 저작물을 암호화하고 저작물 관리시스템에서 세션키와 같이 보관하고 관리하였다. 이런 구조에서 발생 가능한 저작물의 파손 및 변경에 의한 위험요소 즉, 기밀성과 무결성에 대한 문제로부터 저작자의 저작권과 저작물은 보호 받을 수 없다. 이런 문제를 해결하기 위해 백업 관리시스템을 이용한다.

백업 관리시스템의 접근 제어 정책은 정보의 추가 기능만 기본적으로 제공한다. 백업 관리시스템에 접근이 가능한 경우는 일반적으로 두 가지 이벤트가 있다. 새로운 저작물에 대한 생성이 있고, 저작권 이전시 발생하는 이벤트가 있다. 새로운 저작물에 대한 생성은 정상적인 이벤트이므로 저작물을 저작자의 비밀키로 암호화 및 해쉬값을 생성하고 사용된 비밀키와 세션키는 키관리 시스템에 저장한다. 저작권 이전은 저작물에 대한 저작권에 변경을 필요로 한다. 저작권 이전 요청시 기존 자료에 대한 정보 수정은 외부의 불법 접근으로 인한 불법수정의 위험성이 존재하여 기존 저작권 관리번호의 인덱스를 활용하여 수정된 저작권을 추가 등록한다. 이렇게 관리되는 저작물은 저작권 침해 발생 및 법적 공방시 근거자료로 활용된다.

저작물 보안 관리를 위해 두 개의 비밀키를 사용한다. 하나는 네트워크를 통해 등록자와 프로그램 등록 시스템간의 보안 인터페이스를 위한 세션키, 백업 관리시스템에 저작물 저장시 사용된 저작자 비밀키이다. 세션키는 네트워크로 전송되는 저작물을 보호하고 관리 시스템내에서 인가되지 않은자로부터 기밀성 서비스를 제공하는데 활용된다. 그리고 저작물 관리시스템에 저장된 저작물의 무결성을 보장 받기 위해 저작자가 저작물을 동봉하는 암호화키는 저작자 비밀키를 이용한다. 이렇게 저작물을 동봉하여 백업 관리시스템

에 저장함으로서 저작물 관리시스템에서 저작물을 수정 및 파손되었을 때 복구 및 무결성 검증 기능을 제공한다.

(2) 저작권 인증 정책

저작권 전자서명은 모든 저작자가 전자서명 한다. 저작자 N명에 대한 전자서명은 M(SN) = (SKRN(…(SKRU2(SKRU1(Copyright))))와 같이 처리된다. 공동저작자의 인원에 영향을 받지 않고 같은 저장 공간을 요구한다.

예를 들어, "kims", "pol", "davi", "jon"과 같이 4명의 저작권 보호를 위해서는 4명의 전자서명을 필요로 한다.

- SKRkims(copyright) …… ①
- SKRpol(SKRkims(copyright)) …… ②
- SKRdavi(SKRpol(SKRkims(copyright))) …… ③
- SKRjon(SKRdavi(SKRpol(SKRkims(copyright)))) …… ④

①,②,③,④ 각각의 메모리 사이즈는 동일하다. 그러므로 저작권 인증에 필요한 전자서명 메모리 효율성을 가질 수 있다. 또한 20명으로 한정된 공동저작자 인원의 한계를 극복할 수 있다.

(3) 제안시스템 성능 비교

실험 결과, 기존 전자서명은 단일 전자서명의 경우, 783byte의 저장 공간이 필요하다. 또한 다중 전자서명의 경우 "단일 전자서명 * 전자서명인원"의 저장 공간이 활용된다. 실험 시스템의 데이터베이스(오라클 9i)를 활용하여 단일 필드에 하나의 전자서명만을 저장 관리하여 20개 이하의 필드가 필요하다. 실험결과, 제안 시스템은 다중과 단일 전자서명을 구분하지 않고 1Kbyte 이하의 전자서명 필드가 사용된다. Table 1은 성능 분석을 위한 실험 데이터 분석 결과이다.

표 1 저장 공간 성능 비교
Table. 1 Compare the performance of storage space

	User 1	User 2	…	User N-1	User N
기존 전자서명	783byte	783*2 byte	…	783*(N-1) byte	783*N byte
제안 전자서명	783byte	783byte	…	783byte	783byte

제안된 영역 이외에 추가로 3중 DES를 국내환경에 맞도록 SEED 암호화 알고리즘을 활용하였다. Table 2는 기존 프로그램 등록 시스템과 제안 시스템을 성능 분석한 결과이다.

표 2 제안시스템의 성능분석
Table. 2 Performance analysis of system

대상 / 항목	기존 프로그램 등록 시스템	제안 시스템
원본 위·변조 확인	불가능	가능
다중 서명	N개의 개인서명파일	1개의 서명 파일
다중 서명 가능 횟수	20명	제한없음
다중 서명 파일 Size	(단일서명*N개) 파일 Size	단일서명 파일 Size
저작물 무결성 인증 기능	없음	있음
저작물 암호 알고리즘	3DES	SEED
저작물 접근 권한	관리자의 독단적 접근 가능	쌍방 인증에 의한 접근

V. 결론

본 논문에서는 디지털 콘텐츠 시장에서 문제가 되는 프로그램의 불법복제 및 유통으로부터 저작자의 권리를 보호하여 콘텐츠 시장의 활성화를 유도하기 위해 프로그램 저작권 보호를 위한 저작물 및 저작자 인증 시스템을 연구하였다.

제안 시스템은 프로그램 등록시스템을 기반으로 저작자의 저작권과 저작물 보호를 위한 기밀성 및 인증 정책을 적용하였고, 저작권에 대한 법적분쟁발생시 사용자의 요청사항에 대한 부인방지 기능과 등록정보 및 저작물이 원본과 같음을 증명하는 저작물의 신뢰성을 제공한다. 또한 온라인 프로그램 저작물 등록시 공동저작자 인원초과에 대한 한계를 해결하고 메모리 효율성을 높였다.

본 제안 시스템은 프로그램 등록시스템에 등록된 저작물을 저작자 입장에서 저작물의 신뢰성을 보장할 수 있도록 서비스를 제공하여 보다 발전된 형태의 프로그램 등록관리와 디지털콘텐츠 시장을 활성화하는데 기여할 것으로 기대된다.

참고문헌

[1] 박성민, 강석주, 최용락, "프로그램 On-Line 등록 시스템 구축을 위한 설계", 한국인터넷정보학회 춘계학술발표대회논문집, p.105~p.108 2003.

[2] 강석주, 박성민, 최용락, "프로그램 등록시 On-Line을 이용한 지방세 납부의 신뢰성 보장을 위한 사용자 중심의 시스템 설계 및 구현", 한국인터넷정보학회 춘계학술발표대회논문집, p.109~ p.112, 2003.

[3] 강석주, 박성민, 최용락,"프로그램 On-Line 등록시 인증 및 전자지불 연계에 관한 연구", 한국인터넷정보학회 춘계학술발표대회논문집, p.65~p.69, 2003.

[4] 강호갑, "DRM을 이용한 컨텐츠 불법방지사용자시스템 구축 방안", KIEC, 정기간행물, 2001.3.

[5] 강석주, "PKI 보안서비스 기반의 프로그램 저작권 인증시스템 설계", 대전대학교 학위논문, 2004. 8.

[6] M. Mitzenmacher, A. Perrig, Bounds and D. Tygar. Efficients for BiBa Signature Scheme -s, Technical Report, 2002.

[7] 최용락, "상호인증 국제 표준화 동향과 개발사례", 표준화 동향지 -공개키기반구조 표준화- 테마특집, 2000. 4월호.

[8] ISO/IEC 9594-8(1997), Information technology - Open Systems Interconnection - The Directory : Authentication Framework.

[9] IETF RFC 2459(1999), Internet X.509 Public Key Infrastrcture Certificate and CRL Profile.

[10] TTAS.IT-X.509/R2, 디렉토리 시스템 인증 프레임워크 표준.

[11] TTA.KO-12.0001, 부가형 전자 서명 방식 표준 -제2부 : 확인서 이용 전자서명 알고리즘.

저 자 소 개

장 재 혁

2002년 대전대학교 대학원 컴퓨터공학과 석사

2006년 2월 대전대학교 대학원 컴퓨터공학과 박사수료

〈관심분야〉 컴퓨터포렌식스, 지적재산권, 개체인증

이 종 섭

1993년 광운대학교 대학원 전자계산학과 석사

2003년 2월 대전대학교 대학원 컴퓨터공학과 박사수료

2006년 현재 : 한국군사문제연구원 정보통신시스템 IT담당 부장

〈관심분야〉DRM, 문서보안, MGIS

최 용 락

1986년 ~ 현재 : 대전대학교 컴퓨터공학과 정교수

2004년 ~ 2005년 : 대전대학교 교수협의회장

2003년 ~ 현재 : 한국정보보호학회 (충청지부) 고문, 한국정보보호학회 비상임 부회장

2000 ~ 현재 : 대전지방검찰청 컴퓨터수사대 자문위원

〈관심분야〉 모바일 보안, 컴퓨터포렌식스, 접근통제, 지적재산권 보호