# 식별체계와 공개키 기반의 디지털 콘텐트 유통모델 연구

최성원[0]* 이상환* 이상기* 조성남* 석중호*
*한국과학기술정보연구원 정보기술지원실
*{swchoi[0], sanglee, sanggi, chosn, jhsuk}@kisti.re.kr

# A Study on the Digital Content Dissemination Model Based on Identification and Public key

Seong Won Choi[0] S. H. Lee S. G. Lee S. N. Cho J. H. Suk
*Dept. of S&T Information Sysgtem, Korea Institute of Science and Technology Information

**요 약**

최근 급속히 증가하고 있는 Digital Content의 생성과 활용으로 인해 인터넷 기반의 Digital Content 유통이 활성화 되고 있다. 하지만 URL의 한계와 Content의 불법복제 및 무단변형과 같은 역기능이 나타남으로써 양질의 콘텐트 생산·유통이 저해되고 있다. 따라서 본 논문에서는 URN 기반의 DOI 식별체계와 Digital Content 보호를 위한 PKI 기반의 공개키 알고리즘, 그리고 콘텐트 제공자의 저작권을 보호하기 위한 *Digital Watermarking*과 DRM기술을 접목한 강인한 Digital Content 유통모델을 제안하고자 한다.

## 1. 서 론

정보 및 통신 기술의 발달, 초고속 정보통신망의 구축, 멀티미디어 기술의 급속한 발전으로 *Digital Content*(동영상, 정지영상, MP3 등)의 유통에 대한 요구가 급속히 증가하고 있다.

Digital Content는 처리 과정의 단순함과 사용의 편리함 그리고 디지털 통신을 통한 대량 배포의 용이함 등의 장점이 있는 반면 데이터가 갖고 있는 내용의 무결성을 보장하기가 어렵다는 단점이 있다.

디지털 데이터 형식이 다양한 매체에 널리 적용됨에 따라 허가받지 않은 접근에 의한 대량 복제나 저작권자와 상관없는 무단 변형 등으로 컨텐트 소유자들의 저작권을 보장해주지 못하고 있는 상황이다.

따라서, *Digital Content* 제공자는 자신의 노력에 대한 정당한 대가를 받을 수 있으면서 허가되지 않은 사용, 저작권 침해를 방지할 수 있는 기술적, 제도적 환경을 요구하고 있으며, 이러한 환경의 조성은 고급 컨텐츠 생산을 유도하기 위해 필수적이라 하겠다.

본 논문에서는 Digital Content의 식별체계[2,3,4]와 저작권 및 사용규칙의 정의·표현을 위한 메타데이터 그리고 불법적인 사용·복제 방지를 위한 PKI[9,10] 기반의 암호화 방식과 DRM[13], Digital Watermarking[12] 기술을 알아보고 각 요소기술을 접목하여 식별체계[1,5], 공개키 기반의 Digital Content 유통모델을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 식별체계, 암호화 등 관련 연구에 대하여 기술하고, 3장에서는 식별체계와 공개키를 기반으로 한 디지털 콘텐츠 유통모델을 제시한다. 4장에서는 결론과 향후 연구 방향에 대하여 기술한다.

## 2. 관련연구

### 2.1 식별체계 - DOI

현재 인터넷 기반에서 제공되는 Digital Content에 대한 위치정보로 URL을 이용하고 있으나 URL은 Digital Content에 대한 영구적인 식별자로서의 기능을 제대로 수행하지 못하기 때문에 W3C의 IETF는 범세계적으로 유일하게 식별가능하고, 영구적인 식별자로서 URN사양을 정의하였다.

이 사양에 따라 CNRI에 개발을 위탁하여 1997년도에 프랑크푸트의 책 박람회에서 DOI 시스템을 선보인 이 후, 1999년도에 미국표준화 기구인 NISO에서 Z39.84-2000이라는 정식 NISO 표준으로 확정되었다. DOI는 1999년 7월에 W3C의 RFC로 제출되었다[5].

### 2.2 메타데이터 - INDECS Project

INDECS(INteroperability of Data in E-Commerce System) 프로젝트는 Digital Content의 전자상거래를 위한 기반 마련과 지적재산권 관리를 위한 메타데이터가 필요하다는 인식하에 유럽의 Info2000의 지원을 받아 국제저자권협회(WIPO) 등의 국제적인 저작권 소유 기관들의 주도로 1998년 시작되었다[8].

INDECS는 다양한 메타데이터 스키마를 조화시킬 수 있는 공통된 프레임워크로서, 서로 다른 메타데이터 스키마간의 상호운용성 확보를 목표로 한다.

즉 다양한 저작물 및 저작권의 전자상거래 시스템간에 상이한 메타데이터 스키마가 상호 호환되도록 하고 더불어 특정 분야에서 개발된 메타데이터가 다른 분야에서도 이용 가능하도록 하는 것이 주목적이다.

### 2.3 대칭키 및 공개키 암호화 방식

**o 대칭키 암호 알고리즘**

대칭키 암호 알고리즘은 송·수신자가 동일한 키에 의하여 암호화 및 복호화 과정을 수행하는 방식을 일컫는다. Caesar 암호로부터 DES 및 SEED에 이르기까지 2천여평문 배열을 재조정하여 암호화하는 방식이다.

**o 공개키 암호 알고리즘**

대칭키 암호 알고리즘의 최대의 난제는 암호화 과정에서 사용되는 키의 안전한 분배와 전송에 있다. 1976년 W.Diffie와 M.E.Hellman이 최초로 제시한 공개키 암호방식은 기존 암호학의 상식을 뛰어넘는 혁신적인 발상으로 키의 일부를 공개함으로써 키 관리의 어려움을 해결하고자 하는 방식이다[11].

**o 공개키 기반구조(PKI)**

전자서명기술의 기반기술은 공개키 암호알고리즘으로 비밀키와 공개키가 사용된다. 공개키 암호알고리즘에서 사용되는 비밀키가 전자서명을 생성하는 생성키가 되고 공개키가 전자서명을 검증하는 검증키 역할을 한다.

공개키는 공개된 정보이므로 어떻게 공개키 위·변조 문제를 해결하는가 하는 공개키 인증문제로 귀착하게 된다. 이러한 공개키의 인증문제를 해결하기 위해 나온 것이 바로 공개키 기반구조(Public Key Infrastructure: PKI)이다[10].

### 2.4 저작권 보호 기술

**o Digital Watermarking**

워터마킹이란 어떠한 멀티미디어 저작물을 보호하기 위하여 여기에 특별한 형태의 워터마크(저작권 정보, 로고, 인감, 일련번호 등)를 감추고 추출하는 모든 기술적 방법을 뜻한다[12].

초기에는 원래의 멀티미디어 저작물 자체에 대해서 은닉시키는 방법을 연구하였지만 현재에는 많은 기술적 변환방법을 이용한 강력한 워터마킹 기술이 개발되고 있으며 해당 저작물에 삽입된 저작권 정보를 추출함으로서 사후에 디지털 정보의 지적재산권을 보호할 수 있는 기술이라 할 수 있다.

**o Fingerprinting**

핑거프린팅 기술은 워터마킹의 확장 기술로 콘텐트의 상거래시 소유자의 정보뿐만 아니라 구매자의 정보도 포함하는 핑거프린팅 정보를 콘텐트에 삽입하여 후에 불법배포가 어느 구매자로부터 시작되었는지 추적할 수 있도록 해주는 기술이다[13].

불법배포자를 추적할 수 있다는 관점에서 핑거프린팅 기술은

부정자 추적기술로도 논의될 수 있다.

**o DRM(Digital Right Management)**

Digital Rights Management(DRM)는 암호화 기술을 이용하여 허가되지 않은 사용자로부터 Digital Content를 안전하게 보호함으로써 콘텐트 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리하는 시스템으로 정의할 수 있다.

DRM의 기술적 특성으로는 Content Encryption, Usage Rule, Persistent Protection, Usage Tracking, Superdistribution 등이 있다[13].

## 3. Digital Content 유통 모델 제안

정보의 디지털화는 불법복제와 배포, 조작 및 유통을 가능하게 함으로써 저작권자에게 경제적 손실을 끼치고 더 나아가 Digital Content 유통 활성화를 저해하는 원인이 되고 있다.

따라서 불법복제로부터 저작권자를 보호하고 신속한 권한처리 및 투명한 비용배분을 지원할 수 있는 강인한 유통 시스템 연구는 필수적이라 하겠다.

본 장에서는 DOI, INDECS[8], PKI 기반의 공개키 알고리즘[11], 비대칭키 알고리즘, DRM 및 Digital Watermarking 기술을 접목한 강인한 Digital Content 유통 모델을 제안하고자 한다.

### 3.1 Digital Content 유통시스템

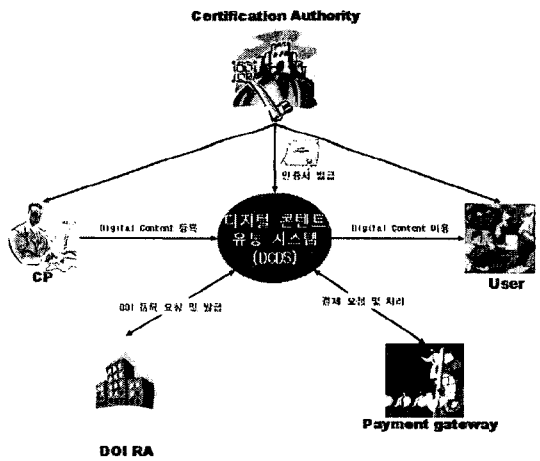


그림 1 Digital Content 유통 시스템 개념도

그림 1은 본 논문에서 제안하고자 하는 Digital Content 유통 시스템(DCDS : Digital Content Dissemination System)의 개념도이다. 상세한 기능을 정의하기에 앞서 전체적인 Digital Content 유통의 흐름을 제시하고자 한다. 먼저 CP는 CA를 통해 발급받은 인증서를 통해 DCDS에 로그인하고 자신이 저작한 콘텐트의 상세 정보 및 사용 규칙(usage rule), 콘텐트를 등록한다.

DCDS는 등록된 콘텐트에 유일한 식별자인 DOI를 부여하기 위해서 DOI RA에 DOI 등록 요청을 하고 DOI를 발급받는다. DCDS는 콘텐트에 CA로부터 받은 인증서를 이용해서 전자서명을 하며 내부적인 암호 및 보호를 위한 process(Digital Watermarking, Fingerprinting, 공개키, 비대칭키 암호화)를 거친 후 이용자 서비스를 준비한다.

이용자는 검색을 통해 콘텐트를 발견하고 DCDS에 이용 요청을 하기 위해 인증서를 이용해서 로그인하게 된다. 콘텐트의 비용을 지불하기 위해 사용자는 DCDS에 결제 요청을 하고 DCDS는 외부 금융기관인 Payment Gateway를 통해 결제를 승인 받게 된다.

최종적으로 DCDS는 Digital Content에 대한 결제 및 사용 통계 등을 관리하며 모니터링 시스템을 통해 주기적으로 콘텐트의 불법유통 여부를 체크하게 된다.

### 3.2 DCDS 주요 기능

Digital Content 유통 모델은 Digital Content Management System(DCMS)과 Digital Content Protection System(DCPS), Clearing House로 구성되어진다.

#### 3.2.1 DCMS (Digital Content Management System)

DCMS은 상호운용성을 위한 통일된 관리체계 기반을 마련하기 위한 시스템으로 주요 기능은 Digital Content의 식별번호(identification) 등록 및 관리, 메타데이터 생성(description), 규칙 설정(rule-setting)이며 다음과 같이 적용된다.

디지털 콘텐트를 식별할 수 있는 고유번호 생성을 위해 신뢰성 있는 DOI RA를 통해 DOI를 부여받고 DOI, 타이틀, 초록, 저작자 정보, 저작권자 정보, 출판 날짜 등과 같은 콘텐트의 세부 정보 및 저작권 정보를 메타데이터 형식에 맞게 저장한다.

저작자는 자신이 창작한 콘텐트에 대한 사용 규칙을 정의하여 등록하게 되며 정의된 규칙은 권리명세언어의 표준인 XRML[6]을 통해서 사용자와 상호 작용된다.

#### 3.2.2 DCPS (Digital Content Protection System)

DCPS은 DCMS을 거친 후 그에 따른 규칙이 실행되는 것을 보장하기 위한 방법으로 콘텐트를 보호하는 시스템이다. 주요 기능은 콘텐트의 암·복호화(encryption), Digital Watermarking , Fingerprinting이다.

CP는 DCMS을 통해 콘텐트에 대한 세부정보와 사용 규칙을 등록하고 최종적으로 서비스될 Digital Content를 서버로 전송하게 될 것이다. 이 때 콘텐트의 보호를 위해 CP는 DCPS의 공개키로 암호화된 콘텐트를 전송하게 되며 암호화된 파일은 DCPS의 개인키를 이용해서 복호화가 이루어진다. 복호화가 끝난 콘텐트는 부여받은 DOI를 Watermarking 한다.

이용자의 구매 및 사용 요청에 따라 요청한 사용자의 개인정보를 Fingerprinting 한 후 세션키(대칭키)를 생성해서 암호화하고 암·복호화의 속도를 고려하여 구매자의 공개키로 세션키(비밀키)만을 암호화해서 서비스 하게 된다.

#### 3.2.3 Clearing House

이용자가 콘텐트를 사용하기 위한 Application 지원, License 생성 및 발급, 과금 및 결제, 통계, 모니터링의 역할을 하는 시스템이다.

콘텐트를 요청한 이용자의 신원확인과 동시에 콘텐트를 이용할 수 있는 플러그인 형태의 user application을 이용자의 PC에 설치하게 한다. DCPS에서 모든 암호화가 끝난 콘텐트를 다운로드 받게 하고 Clearing house에서는 콘텐트에 대한 license를 생성·발급한다.

또한, 콘텐트의 이용 내역과 지불 정보등의 통계 정보를 저장하고 웹 검색엔진과 유사한 기능의 모니터링 시스템을 통해 주기적으로 콘텐트의 불법유통 여부를 체크한다.

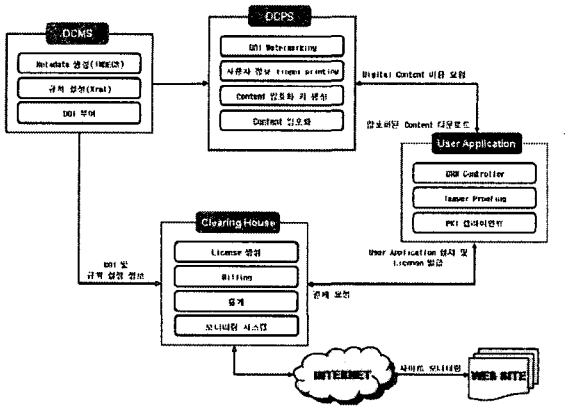


그림 2 DCDS의 내부 처리 구성도

### 3.3 유통 모델의 적용

3.2에서 DOI, PKI 기반의 Digital Content 유통 모델의 전체적인 흐름과 세부적인 기능을 정의하였다. 본 절에서는 제안하고자 하는 유통 모델의 전체적인 프로세스를 순차적으로 살펴보도록 하겠다.

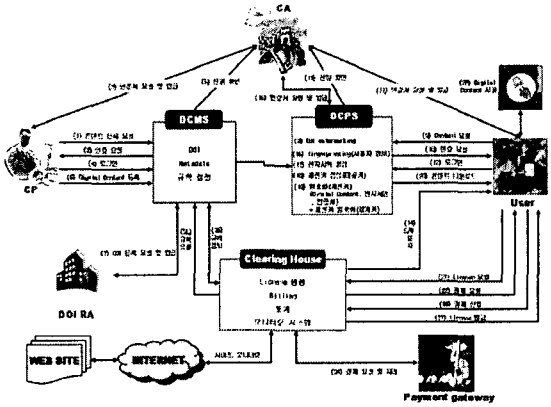


그림 3 전체 구성도

(1) 콘텐트 등록 요청
CP가 소유하고 있는 콘텐트를 등록하기 위해 등록 요청
(2) 인증요청
DCMS는 CP의 신분확인을 위해 인증 요청
(3) 인증서 요청 및 발급
CA에 인증서 요청 및 발급
(4) 로그인
인증서를 이용한 로그인(DCMS)
(5) 신원 확인
CA에 신원 확인 요청
(6) Digital Content 등록
Digital Content의 세부 정보와 사용 규칙 등록(등록된 정보는 DCMS의 공개키로 암호화)
(7) DOI 등록 요청 및 발급
Digital Content에 DOI를 부여
(8) DOI Watermarking
Digital Content에 DOI Watermarking
(9) Digital Content 요청
DCPS로 Content 요청정 전송
(10) 인증 요청
신분확인을 위해 User에게 인증 요청
(11) 인증서 요청 및 발급
인증 확인 위해 CA에 인증서 요청 및 발급
(12) 로그인
인증서를 이용한 로그인(DCPS)
(13) 신원확인
CA에 신원 확인 요청
(14) Plug-in S/W 설치
확인된 User에 대해서 전용 application 설치 알림
(15) 결제 요청
Clearing House의 빌링시스템에서 결제 요청
(16) 결제 신청
결제요청 수락 및 결제 신청
(17) 결제 요청 및 처리
해당 Digital Content에 대한 비용 처리
(18) Fingerprinting(사용자 정보)
결제 처리가 완료 후 사용자 개인정보 Fingerprinting
(19) 인증서 요청 및 발급
Digital Content를 암호화하고 전자서명을 첨부하기 위해 인증서 요청 및 발급
(20) 전자서명 생성
User의 공개키로 암호화한 전자서명 생성
(21) 세션키 생성(대칭키)
(22) 암호화(세션키) + 세션키 암호화
세션키를 User의 공개키로 암호화
(23) Digital Content 다운로드
User의 전용 application에 다운로드
(24). License 요청
license를 Clearing House에 요청
(25) 규칙 요청
User가 구매한 Digital Content의 사용 규칙 요청
(26) 규칙 통보
규칙정보 및 DOI 통보
(27) License 발급
(28) Digital Content 사용
license에 포함된 사용 규칙에 따라 Digital Content를 사용
(기타) 모니터링 시스템
구매된 Digital Content의 사용이 정당하게 이루어지고 있는지, 그리고 저작권이 적절하게 보호되고 있는지 파악

## 4. 결 론

인터넷 환경에서 유통되는 Digital Content는 위치 및 내용이 수시로 변경되어 접근 및 이용 시 많은 어려움이 발생하고 불법 복제 및 조작이 용이하여 저작자의 지적 권리 보호가 매우 어려운 실정이다.

따라서, 본 논문에서는 디지털 정보자원에 대한 고유한 식별기호를 부여하는 기법인 DOI를 이용해서 Digital Content의 접근 효율성 및 이용 편리성을 제공하고, 저작권 및 사용규칙의 정의·표현을 위한 메타데이터로서 INDECS, 과금 및 거래 내역 관리를 위한 DRM, 불법적인 접근 및 사용·복제 방지를 위한 PKI 암호화 방식, Digital Watermarking 기술을 이용해서 저작자에 대한 지적 재산권을 보호하여 Digital Content의 전자상거래를 활성화 할 수 있는 Digital Content 유통 모델을 제안하였다.

제안한 유통 모델을 통해 효율적이고 신뢰성 있는 Digital Content의 저작권 보호가 가능할 뿐만 아니라 제3자 및 합법적인 사용자에 의한 불법 복제 및 배포 등의 위험을 크게 줄일 수 있을 것이다.

## 5. 참고문헌

[1] ANSI/NISO, "Syntax for the Digital Object Identifier," Z39.84-2000, 2000.
[2] T. Berners-Lee. "Uniform Resource Locator-RFC1738," 1994. <http://www.w3c.org/Addressing/rfc1738.txt>
[3] R. Moats. "URN Syntax-RFC2141," 1997. <http://ietf.org/rfc/rfc2141.txt>
[4] T. Berners-Lee. "Uniform Resource Identifiers : Generic Syntax-RFC2396," 1998.
[5] DOI handbook <http://www.doi.org/hb.html>
[6] Xrml2.0 spec. <http://www.contentguard.com/xrml.asp>
[7] DublinCore Metadata Initiative. <http://dublincore.org>
[8] G.Rust & M.Bide, "The <indecs> Metadata Framework : Pinciples, model and data dictionary," 2000. <http://www.indecs.org/pdf/framework.pdf>
[9] ITU-T X.509 Information technology - Open Systems Interconnection - The Directory : Public-key and attribute certificate frameworks
[10] S. Chokhani. "Internet Public Key Infrastructure Certificate Policy and Certification Practies Framework-RFC2527," March, 1999.
[11] PKCS#1 v2.0 - RSA Cryptography Standard. <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/>
[12] R.B. Wolfang and E.J. Delp, "A Watermark forDigital Images," in Proc. IEEE Int. Conf. Images Processing, Lausanne, Switzerland, Sep. 1996, pp. 219 - 222.
[13] DRM forum <http://drm.or.kr>