情報保護學會論文誌
第18卷 第6(A)號, 2008. 12

신뢰할 수 있는 디지털 콘텐츠 유통 아키텍처 방안*

홍 승 필[1], 김 혜 리[1†], 이 철 수[2‡]
[1]성신여자대학교, [2]경원대학교

Applied Method to Trusted Digital Content Distribution Architecture*

Seng-phil Hong[1], Hye-ri Kim[1†], Lee ChulSoo[2‡]
[1]Sungshin Women's University, [2]Kyungwon University

요 약

인터넷 기술과 멀티미디어 기능의 발달로 인하여 디지털 콘텐츠는 새로운 성장 산업으로 주목받으며 다양한 경로를 통해 빠르게 보급되고 있다. 한 예로, 국내 디지털 콘텐츠 산업의 매출 규모 또한 2003년 이후 연평균 14.7%의 높은 성장률을 기록하고 있음에도, 정보 공학의 역기능 측면(저작권 침해, 부적합한 콘텐츠의 범람, 명예 훼손과 프라이버시의 침해)이 주요 문제로 대두되고 있다.

본 논문에서는 앞서 제시한 디지털 콘텐츠 유통 시 문제점을 해결하기 위하여 인터넷 환경 내 신뢰할 수 있는 디지털 콘텐츠 유통 아키텍처 (TDCDA)를 제시하였다. TDCDA는 콘텐츠 배포 시 신뢰성 확보와, 디지털 콘텐츠의 무결성 및 저작권 보호 메커니즘을 통한 안전한 콘텐츠 유통 방안을 소개하였고, 마지막으로 TDCDA의 알고리즘과 적용 방안을 제시함으로써, 실 웹 기반의 컴퓨팅 환경 내 활용 방안을 타진하였다.

ABSTRACT

As the innovative internet technologies and multimedia are being rapidly developed, digital content is a remarkable new growth industry and supplied by various channel. For example, domestic sales volume in digital contents marked an annual increase of 14.7% since 2003. Against the merits of digital content distribution, Information reengineering aspects are getting more serious issues in these days such as infringement of copyright, flood of inappropriate content, invasion and infringement of privacy, etc.

In this paper, we are making a suggestion of the TDCDA-Trusted Digital Content Distribution Architecture in order to solve above problems. TDCDA is provided to how well-define and design the trusted path in digital contents distribution in internet environments using a secure distribution mechanism, digital content integrity and copyright protection. Finally, we also proposed the TDCDA algorithm and applicable guidelines for feasible approach in real computing environment.

Keywords : Privacy, Digital Content, Security, Architecture

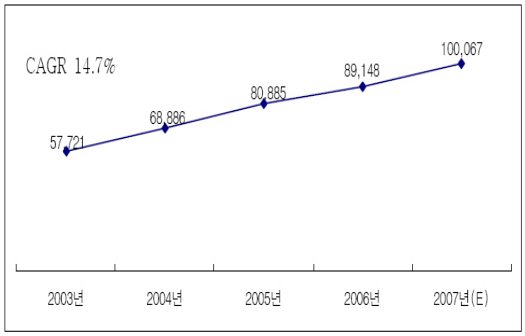
Ⅰ. 서 론

최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사

접수일: 2008년 7월 21일; 채택일: 2008년 10월 7일
* 본 연구는 서울시 산학연 협력사업(NT070103)의 지원으로 수행하였습니다.
† 주저자, philhong@sungshin.ac.kr
‡ 교신저자, csl100@kyungwon.ac.kr

용자 환경으로 변환하고 있다.

정보 통신 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변화하고 있다. 인터넷의 대중화, 무선 네트워크의 활성화, 그리고 모바일 기기의 활용 증대와 함께 다양한 서비스와 디지털 콘텐츠의 융합에 따른 디지털 콘텐츠 서비스 기술이 하루가 다르게 발전하고 있다[1]. 국내 디지털 콘텐츠 산업의 매출 규모는 조사를 처음 시작한 2003년 5조 7,721억원을 기록한 이래 연평균 14.7%의 높은 성장률을 기록하며 2007년에는 10조 67억원에 이른 것으로 나타났다. 이는 이전에 비해 성장률이 크게 둔화된 것으로 나타나고 있으나, 국내 전체 경제 성장률이 4.7%임을 감안하면 여전히 높은 성장세이며 금액적으로 매출 규모 10조원을 돌파하였다는데 의미를 둘 수 있다[2].



(출처:2007년도 국내 디지털콘텐츠산업 시장조사 보고서)

[그림 1] 디지털콘텐츠산업 시장 규모 추이 (2003~2007) (단위 : 억원)

이러한 디지털 콘텐츠 시장의 발전과 더불어 크게 이슈화 되고 있는 것이 바로 콘텐츠 보안이다. 디지털 정보는 여러 번의 복사에도 원본과 동일한 품질 상태를 유지할 뿐만 아니라 초고속망을 통해 광범위한 지역으로 신속하게 배포가 가능하고, 정보의 변경이 용이하다는 특성으로 인해 불법복제 및 위/변조 등과 같은 각종 보안 위협에 쉽게 노출되어 있다[3]. 또한 통방융합, 디지털 홈, 디지털기기의 다기능화 등 디지털 기술의 컨버전스 가속화가 이루어지고 있는 상황에서 디지털 콘텐츠 산업을 보다 활성화하기 위해서는 다양한 콘텐츠 서비스 모델과 사용자 환경을 지원할 수 있는 콘텐츠 보호 기술이 필요하다. 그리하여 DRM을 중심으로 디지털 콘텐츠 보호 방안에 대해 법제 현황과 기술 현황으로 나누어 동향을 알아보고. 신뢰할 수 있는 디지털 콘텐츠 유통 아키텍처를 를 제시함으로써 음란물 및 불법 동영상 유출 관련 대안 방안을 제안하고, 그 활용성을 소개해 보고자 한다.

본 논문의 구성은 다음과 같다. 1장에서는 본 논문의 개요를 소개하고 2장에서는 관련 연구를 분석하였으며 3장에서는 문제점을 도출해 보았다. 4장에서는 신뢰할 수 있는 디지털 콘텐츠 유통 아키텍처에 대한 3가지 메커니즘과 적용방안을 소개하였으며 5장에서는 기대효과를, 마지막으로 6장에서는 결론 및 향후 연구 방안을 제시하였다.

Ⅱ. 관련 연구

2.1 기술 분야

DRM (Digital Rights Management)

DRM(디지털 콘텐츠 권리 관리-Digital Rights Management)은 암호화 기술을 이용하여 디지털 콘텐츠의 지적 자산에 대한 권리를 지속적으로 관리 및 보호하는 기술로, 허가되지 않은 사용자로부터 콘텐츠의 접근 및 이용을 불가능하게 통제하는 수단을 제공한다[4][5].

DRM의 대표 기술인 워터마킹(Watermarking)은 텍스트, 이미지, 비디오, 오디오 등의 데이터에 원 소유주만이 아는 마크(Mark)를 사람의 육안이나 귀로는 구별할 수 없게 삽입하고 이를 네트워크에서 제공한다. 만약 사용자들이 멀티미디어 디지털 정보를 불법 복제하여 정당한 대가나 허락없이 상업용 혹은 기타 용도로 사용되었을 때에는 자신의 '마크'를 추출함으로써 자신의 소유임을 밝힐 수 있다[6][7][8].

PKI(Public Key Infrastructure) · PMI (Privilege Management Infrastructure)

PKI(공개키 기반구조-Public Key Infrastructure)란 개방형 네트워크 또는 분산형 네트워크의 환경 하에서 보안 요구사항을 만족시키기 위하여 사용자가 보유한 암호를 이용하여 거래자의 신원을 확인하는 방식으로, 공개키 알고리즘을 통한 암호화 및 전자서명을 이용한

[표 1] DRM의 기술 요소 및 내용

(출처 : "DRM 표준화 및 평가 기술")

구분	요소기술	세부 요소기술
접근 차단 보호기술	콘텐츠 패키징 기술	콘텐츠 패키징 구조선언 및 파일 포맷설계 기술
		복합콘텐츠 패키징 기술
		콘텐츠 암호화 및 키 관리 기술
	권리표현 기술	권리 데이터 사전
		XML 기반의 동적 사용규칙 권리 표현 기술
		범용 REL 파서 설계 및 구현 기술
		저작권 관계표현과 권리정보 저장 및 관리 기술
	복제방지 기술	디바이스 인증 및 폐기/회복 기술
		비밀키(암호화) 교환 기술
	도메인 내 권한관리기술	디바이스 인증 및 도메인 합류/탈퇴 처리 기술
		Virtual domain 구성 기술
저작권 보호기술	워터마킹/ 핑거프린팅 기술	공모공격에 강인한 워터마킹 기술
		공모허용 실시간 핑거프린팅 삽입기술
		공격 및 평가 기술
연동 및 관리 기술	IPMP 인터페이스 기술	IPMP 표현언어 및 인증처리기술
		Interoperable IPMP 표준인터페이스 설계 구현 기술
		DRM adaption 기술
	콘텐츠 식별체계	식별자 구문구조 및 전환기술
		식별 메타데이터 관리 기술
	DRM 도메인 간 상호연동기술	DRM간 상호 인증 처리 기술
		DRM adaption 기술
		훼손된 DRM 모듈 폐기 처리 기술

다. 즉, 암호화와 복호화 키로 구성된 공개키를 이용하여 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 기반 구조이다. 이는 전자거래나 정보유통의 안전성과 신뢰성을 확보하기 위한 시스템으로, 상대방의 신원을 확인하고 정보 내용의 변경확인과 비밀유지 기능을 갖는 지식 정보화 사회의 핵심기반이다[9][10].

공개키 기반구조에서 사용되는 공개키 인증서는 주로 사용자의 신원 확인 등의 인증 기능을 위해 사용되며 임무, 지위, 역할 등과 같은 다양한 속성(Attribute) 정보에 대한 권한 인증 서비스를 제공하는 데는 한계를 가지고 있다. 그리하여 이러한 점을 보완하기 위해서 PMI(권한관리 기반구조-Privilege Management Infrastructure)와 같은 부가적인 구조가 필요하게 되었다. 여기서 권한관리 기반 구조란 권한 관련 자원과 이의 소유자간의 관계를 신뢰기관이 보증하고 유지하는 구조를 일컫는다[11][12].

2.2 법 · 제도 분야

현재 국내에서는 "저작자의 권리와 이에 인접하는 권리를 보호하고 저작물의 공정한 이용을 도모함으로써 문화의 향상 발전에 이바지함을 목적"으로 저작권법을 시행중이다. 또한 온라인상에서의 디지털 콘텐츠 산업을 육성하기 위해, 온라인디지털콘텐츠산업의 발전에 필요한 사항을 정함으로써 온라인디지털콘텐츠산업의 기반을 조성하고 그 경쟁력을 강화하여 국민생활의 향상과 국민경제의 건전한 발전을 도모하고 있다. 다음 [표 2]는 국내의 디지털콘텐츠산업 관련 법령 현황을 표로 정리한 것이다.

국외 법·제도의 대표적 특징은 디지털 콘텐츠의 유통 경로가 늘어남에 따라 저작권 문제가 중요한 이슈로 대두되었으며 이와 관련해, 불법 복제 방지를 위한 국가의 노력이 아래 [표 3]과 같이 전개되고 있다.

지적재산권의 침해에 대한 국제적인 분쟁은 주로 디

[표 2] 국내 DRM 법 제도 현황
(출처 :디지털 저작권 관리(DRM)-TCI REPORT 2006)

부	근거법	설명
정보통신부	온라인디지털콘텐츠 산업 발전법 (제10조)	· 온라인 콘텐츠의 품질향상과 호환성 확보 등을 위해 온라인콘텐츠에 관한 표준의 제정 · 개정 · 폐지 및 보급과 온라인콘텐츠와 관련된 국내외 표준의 조사 · 연구 · 개발을 추진
문화관광부	문화산업진흥 기본법 (제18조)	· 디지털 문화 콘텐츠의 효율적 개발, 품질향상 및 범용성 확보 등을 위하여 디지털 문화 콘텐츠에 관한 표준의 제정 · 개정 · 폐지 및 보급, 디지털 문화 콘텐츠와 관련된 국내외 표준의 조사 · 연구 · 개발을 추진
	음악산업진흥에 관한 법률 (제9조, 제14조)	· 음반 등의 효율적인 개발 · 품질향상 및 범용성 확보 등을 위하여 음반 등의 표준화를 추진 · 음반 등의 불법복제 · 유통 등을 방지하기 위하여 문화관광부장관이 음반 등의 기술적 보호조치 및 권리관리 정보의 부착을 위해 지원
	게임산업진흥에 관한 법률 (제8조)	· 정부가 게임물의 기술적 보호, 게임물 및 게임물 제작자를 식별하기 위한 정보 등 권리관리정보의 표시활성화를 위해 관련 사업을 추진
산업자원부	이러닝(전자학습) 산업발전법(제11조)	· 이러닝 산업의 발전을 위하여 이러닝에 관한 표준의 제정 · 개정 · 폐지 및 보급, 이러닝과 관련된 국내외 표준의 조사 · 연구 및 개발, 그 밖에 이러닝의 표준화에 관하여 산업자원부령이 정하는 사업을 추진

[표 3] 디지털 콘텐츠 분야별 각 국가 정책
(출처 : MBAP-2006)

국가	주요 내용
미국	· DMCA 법안을 통해 지적재산권 보호
프랑스	· 2006년 DRM 및 저작권 침해와 관련, DADVSI 법안 도입
일본	· 지적재산권추진계획 2006을 통해 창작자 권리 보호
중국	· 2006년 7월부터 온라인 저작권 보호 법안 발효

지털 콘텐츠 산업이 강세를 보이는 선진국을 중심으로 제기되고 있으며 개발도상국의 경우 아직 관련 정책 마련이 미비한 상황이다.

2.3 표준화 동향

DRM의 표준화가 본격적으로 거론되기 시작한 시점은 2000년 초부터라고 할 수 있다. 당시 인터넷의 급속한 확산과 온라인 음악 및 e-Book의 전자상거래가 새로운 디지털 콘텐츠 산업의 수익원으로 부상하게 되자 많은 DRM 제품이 시장에 출시되었다. 그러나 DRM 업체들은 각각 고유한 기술을 이용하여 제품을 내놓았기 때문에 제품 간의 호환성이 제공되지 않았다. MPEG- 21, OeBF, SDMI 등은 DRM 제품간 상호호환성이 갖추어지지 않고는 시장의 활성화가 어렵다고 판단되어 DRM의 표준화를 위해 설립된 국제적 표준화 단체이다[3].

[표 4] DRM 표준화 진행 현황

기술 분야	표준 단체	활동 내용
Copy Protection	CPTWG	DVD, 디지털방송 분야의 복제방지기술 표준화 포럼
	Smart Right	디지털 홈 환경에서의 디지털콘텐츠 복제방지 기술
	SVP	디지털 홈 환경에서의 디지털콘텐츠 복제방지 기술
	AACP	HD DVD의 복제방지 기술
	OpenCable CPT	케이블방송의 복제방지기술 표준
	4C CPPM/ CPRM	저장장치에 저장되는 디지털 콘텐츠의 복제방지 기술
	5C DTCP	디지털전송채널을 통해 디바이스 간에 전송되는 디지털 콘텐츠의 복제방지기술
	HDCP	디지털 디스플레이 장치로 전송되는 디지털 영상신호의 복제방지 기술
	DVD CCA	DVD의 복제방지 기술
CAS	NGNA	차세대 디지털케이블 기술규격 개발
	DVB CA	디지털방송 콘텐츠의 보호를 위한 수신권한제어(CA) 기술
	ATSC CAS	지상파 디지털방송 콘텐츠의 수신권한제어(CA) 기술

DRM 표준화는 표준단체별 성격에 따라 다양한 분야의 DRM 기술들을 다루고 있는데, 크게 DRM 플랫폼과

권리표현기술(REL : Rights Expression Language), Meta data, 복제방지 기술(Copy Protection), 그리고 CAS 기술 분야로 구분된다[5][6].

본 논문에서는 다양한 DRM 기술 중 매체 보안과 콘텐츠의 소유권, 그리고 향후 발 생할 수 있는 사고를 대비한 책임 추적성과 관련된 복제방지 기술과 CAS 기술의 현황을 중점적으로 알아보고 아래와 같은 표로 정리하였다. 복제방지 및 CAS 기술은 최근 국내의 디지털 방송과 IPTV 기술의 발전으로 그 필요성이 대두되고 있으나 아직은 해외에 의존하고 있는 상태이므로 기술 개발이 필요한 부분이다. 본 연구에서는 디지털 콘텐츠의 복제방지 기술을 중심으로 연구를 진행하였다.

Ⅲ. 문제점

3.1 법/제도적

아이디 공유 및 P2P를 통한 파일 공유 등 저작권 침해 사례에 대해 P2P 및 웹 스토리지 업체에 대한 모니터링 강화 및 단속 강화, 공인인증서의 도입으로 사용자 신분 확인, 저작권 법 적용 등의 구체적인 대책이 필요하다. 또한 많은 콘텐츠에 대한 수작업의 모니터링이 아닌 관리자들에게 명확한 책임과 역할을 주어 확실한 사전 검토를 할 수 있는 구체적인 방안을 마련해야 한다.

3.2 기술

디지털 콘텐츠의 형태와 적용 분야가 다양하며 디지털 콘텐츠의 각 유통 주체들이 서로 다른 특유의 DRM 기술을 제안 및 적용하기에 시스템 간 호환성이 요구된다. 이는 디지털 컨버전스의 가속화가 이루어지고 있음에도 불구하고 서비스별, 기기별, 업체별로 상이한 기술 규격의 DRM을 사용함에 디지털 콘텐츠 산업을 활성화하는데 있어 최대 걸림돌로 작용하고 있다. 현재 콘텐츠 제공자가 콘텐츠 및 기기별로 DRM을 따로 제공하거나 제조업체가 복수 개의 DRM 클라이언트를 탑재하는 등으로 개발이 진행되고 있지만, 이는 관리 및 비용 등의 문제뿐만 아니라 각 DRM 간의 충돌로 인한 시스템 불안정을 초래할 수 있는 문제점을 지니고 있다.

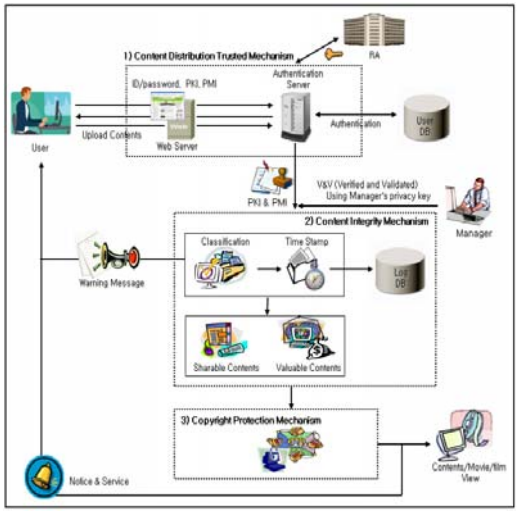
위와 같은 문제점의 해결 방안으로써 본 논문에서는 신뢰할 수 있는 디지털 콘텐츠 배포 시스템을 제안 해보았다. 시스템은 콘텐츠 배포 시 콘텐츠를 제작한 사람의 소유권과 저작권을 보호할 수 있는 측면과, 불법 콘텐츠의 유통 방지에 대한 기술적 제안의 2가지 측면에서 고려되었다. 그리하여 콘텐츠 배포에 대한 책임 추적성을 확보하고, 일어날 수 있는 사고에 대한 법적 기반의 디지털 포렌식 기술을 적용할 수 있게 함으로써 콘텐츠 배포에 대한 신뢰성을 높일 수 있는 방안을 연구하였다.

Ⅳ. TDCDA (Trusted Digital Content Distribution Architecture)

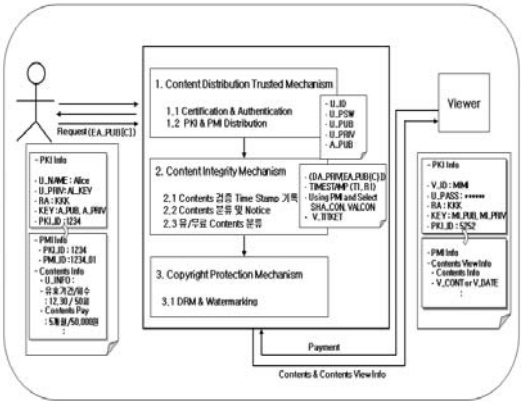
4.1 TDCDA

불법·유해 콘텐츠가 무방비로 노출되는 환경에서 안전한 콘텐츠의 유통을 위한 TDCDA(Trusted Digital Content Distribution Architecture)의 구성은 1) 콘텐츠 배포 신뢰성 메커니즘(Content Distribution Trusted Mechanism), 2) 콘텐츠 무결성 메커니즘(Content Integrity Mechanism), 3) 저작권 보호 메커니즘(Copyright Protection Mechanism)이며 아키텍처는 아래 [그림 2]와 같다.

디지털 콘텐츠를 업로드 하고자 하는 사용자는 신분 확인 후, 등록 과정에서 취득 한 관리자의 공개키를 통해 암호화하여 콘텐츠를 업로드 한다. 관리자는 콘텐츠를 배포하기 전 암호화된 콘텐츠를 관리자의 비밀키를



[그림 2] TDCDA 구성도



[그림 3] Trusted Digital Content Distribution Model

이용하여 복호화 한 후 콘텐츠를 확인하며, 이때 콘텐츠 내역에 대한 모니터링과 동시에 관리자의 로그 기록이 남게 된다. 이는 관리자의 책임을 명확히 하고 추후 혹시 발생할 수 있는 사건·사고에 대하여 책임 추적을 할 수 있게 하여 유해 콘텐츠의 업로드를 사전에 방지한다. 다음 [그림 3]은 신뢰할 수 있는 디지털 콘텐츠 유통 모델을 나타낸 것이다.

4.1.1 콘텐츠 배포 신뢰성 메커니즘 (Content Distribution Trusted Mechanism)

사용자가 콘텐츠를 업로드하기 위해서는 우선적으로 사용자 등록이 이루어져야 한다. 이때, 콘텐츠 배포 신뢰성 보호 메커니즘(Content Distribution Trusted Mechanism)

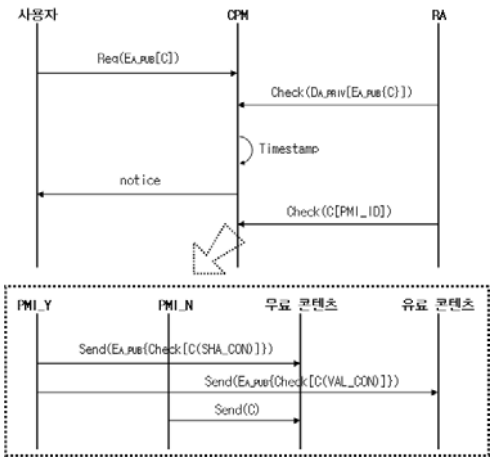
[그림 4] 인증서 확장 필드 적용 예

을 기반으로 사용자 신분 인증 절차를 거치게 된다. 아래 [그림 4]는 X.509 V3.0 인증서를 통한 암호화 기반의 신분확인 후 개인정보 정책 및 저작권법에 준한 사용자의 적합한 속성을 확장 필드를 활용하였을 때의 예시이다.

사용자는 자신의 정보 및 ID/PW를 사용자 인증 서버에 전송하여 등록을 요청하면 사용자 인증 서버는 요청된 사용자의 신분을 확인한다. 신분 확인 후 저작권 보호 및 무료/유료 콘텐츠 업로드 시 필요한 속성인증(PMI)을 등록기관(RA)에 요청한다. 신분 확인을 마친 사용자에 한해 속성인증(PMI)과 관리자의 공개키를 보내어 사용자에게 등록을 마쳤음을 알린다.

4.1.2 콘텐츠 무결성 메커니즘(Content Integrity Mechanism)

신분 확인된 사용자가 제공한 콘텐츠가 배포되기에 적합한지 검증하는 메커니즘이다. [그림 5]는 등록을 마친 사용자의 콘텐츠 업로드 과정을 보여준다.



[그림 5] 콘텐츠 무결성 메커니즘 절차

E : 암호화 C : 콘텐츠 D : 복호화 A_PUB : 관리자의 공개키, A_PRIV : 관리자의 개인키, SHA_CON : 무료 콘텐츠, VAL_CON : 유료 콘텐츠.

먼저 사용자 인증서버는 사용자의 신분을 확인 후 콘텐츠를 콘텐츠 무결성 메커니즘으로 전송한다. 이때의 콘텐츠는 관리자의 공개키로 암호화 되어 있다.

관리자가 암호화된 콘텐츠를 자신의 개인키로 복호화 하여 콘텐츠 확인 작업을 거친다. 이 때 관리자가 콘텐츠를 확인했음을 증명할 수 있도록 모니터링과 동시에 타임스탬프 기능을 활용하여 DB에 로그기록을 남긴

[표 5] PMI 활용 예시

```
<xsd:schema>
<ElementType name='PMI' content='mixed'>
<!--소유자 정보-->
        <Element type='holder'>
        <element type='U_ID'/>
        <element type='U_NAME'/>
        </Element>
<!--발급자 정보-->
        <Element type='issuer'>
        <element type='issuerName'/>
        <element type='baseCertificateID'/>
        </Element>
<!--속성인증구별번호-->
        <Element type='PMI_ID'/>
<!--확장필드 적용 방안-->
        <Element type='attr'>
        <element type='contentPay'>
        <AttributeType name='con_pay'/>
        </element>
        <element type='contentExpire'/>
        </Element>
</ElementType>
</xsd:schema>
```

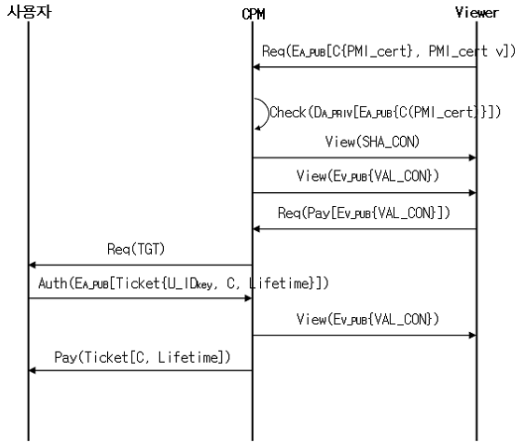
```
<?xml version="1.0" encoding="euc-kr" ?>
<PMI>
        <holder>
                <U_ID>1234</U_ID>
                <U_NAME>Alice</U_NAME>
        </holder>
        <issuer>
                <issuerName>RA</issuerName>

<baseCertificateID>RA_1</baseCertificateID>
        </issuer>
        <PMI_ID>
                1234_01
        </PMI_ID>
        <attr>
                <contentPay con_pay=
 'VAL_CON'>
                50,000 Won
                </contentPay>
                <contentExpire>
 5 Months
 </contentExpire>
        </attr>
</PMI>
```

다. 이는 향후 발생할 수도 있는 사건·사고에 대비하여 관리자에게 유해 콘텐츠의 유포 책임을 추적할 수 있는 기능을 제공한다. 콘텐츠 확인 시 적합하지 않은 유해 콘텐츠일 경우 사용자에게 콘텐츠의 업로드가 제한되었음을 알리고 경고 메시지(Notice기능)를 함께 보낸다.

모니터링을 거친 콘텐츠는 PMI 속성 값 여부에 따라 콘텐츠를 분류한다. PMI 속성 값을 사용함으로써 기업이나 개인의 정보와 콘텐츠 정보 등의 속성이 함께 기록되고 이는 개인 또는 기업이 저작권 및 유·무료 콘텐츠를 적용할 때 유용하다. 개인 및 기업의 이익과 저작권 보호를 위한 유료 콘텐츠는 별도로 분류한다. 아래 [표 5]는 PMI의 속성 값을 XML로 적용한 예시이다.

4.1.3 저작권 보호 메커니즘 (Copyright Protection Mechanism)

DRM과 PKI Extension Fields를 활용하여 콘텐츠 소유권자 및 콘텐츠의 저작권을 보장하고 콘텐츠 무단 복제를 방지하는 메커니즘이다. DRM 적용 시 용량이 다소 큰 동영상 콘텐츠에 대해서는 전체에 워터마킹 기술을 적용하기에는 무리가 있으므로 selection field 값을 이용하여 마크(Mark)를 삽입하고 저작권을 보호 한다. 만약 불법 복제나 정당하지 않은 접근, 허락 없이 콘텐츠를 이용하게 되었을 때 소유자는 마크를 추출함으로써 자신이 소유자임을 밝힐 수 있다.



[그림 6] 저작권 보호 메커니즘 절차

PMI_cert U : 콘텐츠 제공자의 PMI 인증서, V : 콘텐츠 이용자, Ticket : 일정기간 동안 권한 부여, AUTH : 권한부여 승인.

또한 속성 인증서를 이용하여 무료 콘텐츠와 유료 콘텐츠를 식별하고, 정당한 대가를 지불한 이용자만이 콘텐츠를 이용할 수 있게 한다. 유료 콘텐츠 중에서도 이용 횟수 혹은 시간에 제한이 있는 콘텐츠를 식별하여 정해진 기간이 지난 후에는 이용을 제한 할 수 있다. 다음 [그림 6]은 유·무료 콘텐츠 이용 과정을 보여준다.

4.2 TDCDA 적용 방안

아래 [표 6]은 TDCDA에 관한 표기법을 정의하고 실제 적용 예제를 통하여 TDCDA를 증명해 보았다.

· *사용자는 콘텐츠의 등록을 위해 시스템에 사용자 등록 요청을 한다. 사용자 등록 시 필수 정보와 부가 정보를 입력 후, 요청이 승인되면 시스템은 사용자에게 키 값을 발부하고 등록 요청이 승인됨을 알린다.*

1. 사용자“U”는 등록 요청을 한다.
   1.1 사용자 “U”는 필수정보 <U_ID, U_PWD, U_INFO>를 입력한다.
   1.2 부가정보로 PMI 콘텐츠에 관련된 속성정보 <PMI_ID, U_NAME, CON_PAY, CON_EXPIRE>를 입력 한다.
   1.3 요청 승인 후, RA는 PKI&PMI 기반의 키 <U_PRIV, U_PUB>를 부여한다.
   1.4 사용자“U”에게 등록 요청이 승인 되었음을 알린다.
   1.5 만약 사용자 “U"가 적합하지 않은 사용자라면 등록 거부 메시지를 전송 한다.

· *사용자는 등록하고자 하는 콘텐츠의 업로드를 위해 시스템에 로그인 후, 업로드 하고자 하는 콘텐츠를 관리자의 공개키로 암호화 후 전송한다. 관리자는 전송받은 콘텐츠를 개인키로 복호화하여 확인하며, 이 때 최초 확인자가 누구이며 시간이 로그 DB에 기록된다. 확인 한 콘텐츠가 적합하지 않으면 Notice를 보내고 업로드를 사전에 차단한다.*

2. 사용자“U”는 콘텐츠“C” 업로드를 요청 한다.
   2.1 사용자“U”는 등록된 <U_ID, U_PWD>로 로그인을 한다.

[표 6] TDCDA 표기법

Notation
U : 콘텐츠 제공자
A : 관리자
V : 콘텐츠 이용자
C : 콘텐츠
E : 암호화
D : 복호화
U_ID : 콘텐츠 제공자의 ID
U_PWD : 콘텐츠 제공자의 Password
U_INFO : 콘텐츠 제공자의 신상정보
U_NAME : 콘텐츠 제공자의 NAME
V_ID : 콘텐츠 이용자의 ID
V_PWD : 콘텐츠 이용자의 Password
V_INFO : 콘텐츠 제공자의 PMI 속성값
CON_PAY : 콘텐츠에서 무료/유료를 알 수 있는 속성
SHA_CON : 무료 콘텐츠
VAL_CON : 유료 콘텐츠
CON_EXPIRE : 콘텐츠 만기일
U_PRIV : 콘텐츠 제공자의 개인키
U_PUB : 콘텐츠 제공자의 공개키
A_PRIV : 관리자의 개인키
A_PUB : 관리자의 공개키
V_PRIV : 콘텐츠 이용자의 개인키
V_PUB : 콘텐츠 이용자의 공개키
Sig U : PKI와 PMI로 승인된 key 분배
t1 : 콘텐츠 검증 시각
t2 : 콘텐츠 업로드 시각
r1 : 임의 생성 숫자
Action : request / response / check / monitoring / timestamp / notice / warning / upoad / login / view
PKI_cert U : 콘텐츠 제공자의 PKI 인증서
PMI_cert U : 콘텐츠 제공자의 PMI 인증서
Ticket : 일정기간 동안 소유자가 콘텐츠의 권한을 요청자에게 부여
TGT : Ticket-granting Ticket

   2.2 사용자“U”는 업로드 하고자 하는 콘텐츠 “C”를 관리자 공개키A_PUB로 암호화 하여 관리자 “A”에게 Req(EA_PUB[C])로 전송한다.
   2.3 관리자“A”는 전송 받은 콘텐츠“C”를 관리자 “A”의 개인키 A_PRIV로 복호화 하여 적합한 콘텐츠인지 Check(DA_PRIV[EA_PUB{C}])로 확인한다.
   2.4 관리자 확인과 동시에 PKI기능인 Timestamp를

활용하여 <U, A, t1, r1, Action, PKI_cert U, PMI_cert U >으로 로그DB에 기록한다.

2.5 적합한 콘텐츠가 아닐시, 사용자“U”에게 notice message와 함께 업로드를 차단 한다.

2.6 콘텐츠“C”의 PMI_cert U 여부 및 속성 CON_PAY를 이용하여 무료/유료로 분류한다.

· *검증된 콘텐츠에 저작권 보호를 위한 기술을 적용한다.*

3. 콘텐츠“C”에 저작권보호를 위해 기술을 적용 한다.

3.1 관리자 “A”에 의해 검증된 콘텐츠를 특정정보 <C, U_ID, CON_PAY, CON_EXPIRE>를 이용하여 워터마크 WaterMark(EA_PUB[C{U_ID, CON_PAY, CON_EXPIRE}])를 생성 한다.

3.2 워터마킹 기술을 이용하여 워터마크를 삽입한다.

· *콘텐츠를 Viewer 들이 이용할 수 있도록 웹에 게시한다.*

4. 사용자“U”의 요청을 수락하여 콘텐츠“C”를 웹에 게시한다.

4.1 관리자는 최종 콘텐츠“C"를 웹에 게시 한다.

· *게시된 콘텐츠를 이용하기 위한 이용자는 이용 요청을 하고, 콘텐츠의 속성값을 이용하여 유/무료 여부 및 이용자의 권환 확인 후 적합한 이용자에게 콘텐츠*를 이용할 수 있도록 허가한다.

5. 게시된 콘텐츠“C”를 이용자“V”가 이용한다.

5.1 이용자“V”가 시스템에 사용자 등록을 한다.

5.2 이용자“V”가 선택한 콘텐츠“C”의 이용 요청을 한다.

5.3 콘텐츠“C”의 유/무료를 확인 후, 유료 “C"에 Pay(EV_PUB[C{VAL_CON}]) 한다.
TDCDA가 이용자“V”가 요청한 콘텐츠“C”에 대한 권한이 없을 경우 사용자“U”에게 TGT를 요청한다.

5.4 요청 받은 사용자“U”는 Ticket을 암호 화하여 EA_PUB[Ticket(U_IDkey, C, Lifetime)] 전송한다.

5.5 Ticket으로 권한을 승인 받은 TDCDA는 이용자 “V”의 권한을 확인한 후, 콘텐츠 “C”를 제공한다.

다음 [표 7]은 TDCDA를 일반적인 알고리즘의 모습으로 정형화한 것이며 크게 3가지의 함수를 이용하여 나타낸 것이다.

[표 7] TDCDA 알고리즘

1. Function *U_request_ Registration*
// 콘텐츠를 등록하고자 하는 이용자 U의 등록 요청
1.1 U_Mandatory_Input = <*U_ID, U_PWD, U_INFO, request*> // 필수 입력 사항
1.2 U_Option_Input = <*PMI_ID, U_NAME, CON_PAY, CON_EXPIRE*>
// 부가 정보 입력사항
1.3 Send_to Sig U = <Key_Distribution(U_PRIV, U_PUB)>
1.4 IF Sig U is valid
THEN Send_to_U = Notice(msg“Registration OK”)
1.5 ELSE Send_to_U = Notice(msg“Rejection”)

2. Function U_request_Upload
// 콘텐츠를 업로드 하는 과정
2.1 Check U_Input = <*U_ID, U_PWD, login*>
// 이용자 로그인
2.2 Send U_upload_C = <*U_ID, C, upload, t2, PMI_cert u*>
// 등록하고자 하는 콘텐츠의 전송
Input <EA_PUB(U_upload_C)>
2.3 Check C = Monitoring<DA_PRIV (EA_PUB [U_upload_C])>
// 관리자의 콘텐츠 사전 확인
At once,
2.4 Record log_Timestamp = <U, A, t1, r1, upload, PKI_cert u, PMI_cert u>
2.5 IF Check_C is not suitable,
// 적합하지 않은 콘텐츠에 대한 경고
THEN Send_to_U = Notice(msg “Upload Rejection”) and Suspend_upload_C
ELSE
THEN next step
2.6 IF Check_DA_PRIV(PMI_cert u(PMI_ID)) is not valid
// 검증된 콘텐츠에 대한 유/무료 확인
THEN Divide SHA_CON
ELSE
IF DA_PRIV(PMI_cert u(PMI_ID)) is valid
THEN
IF PMI_cert u(CON_PAY) is valid
// 유료 콘텐츠의 경우
THEN Divide VAL_CON

```
        ELSE // 무료 콘텐츠의 경우
            THEN Divide SHA_CON

3. Function C_Copyright_Protection
   // 허가받은 콘텐츠의 저작권 보호를 위한 과정
 3.1 Content = <C, U_ID, CON_PAY,
                CON_EXPIRE>
 3.2 Create WaterMark_Content =
     <EA_PUB(Content)>
     // 저작권 보호를 위한 WaterMark 삽입
     Insert Protection_Content =
                    <C(WaterMark_Content)>

4. Function Web_upload
   // 검증된 컨텐츠의 웹 사이트 업로드
 4.1 U_Output = <Protection_Content, U_ID,
                 t2, upload>

5. Function C_view
   // 콘텐츠를 이용하고자 하는 사용자의 콘텐츠를
   보기 위한 과정
 5.1 Check V_Input =
                        <V_ID, V_PWD, request>
     // 콘텐츠를 이용하고자 하는 사용자의 등록
 5.2 Reqest V_Content=
          <EA_PUB(C{PMI_cert}, PMI_cert v)>
     // 콘텐츠 이용에 대한 요청
 5.3 Check C(CON_PAY)
     // 콘텐츠의 유/무료 확인 과정
     IF C(CON_PAY) = SHA_CON
                  // 유료 콘텐츠에 대한 권한 획득 과정
               THEN V_View = <C(SHA_CON)>
     ELSE
     IF C(CON_PAY) = VAL_CON
     TEHN Pay =
                     <EV_PUB[C(VAL_CON)]>
 5.4 IF TDCDA_authority is not V_Content
         THEN TDCDA_Request = TGT
 5.5 Send U_response_TICKET =
     <EA_PUB[Ticket(U_IDkey, C, Lifetime)])>
     View V_View = <EV_PUB(VAL_CON)>
```

Ⅴ. 기대 효과

TDCDA는 아래와 같이 크게 3가지의 효율성을 추정할 수 있다.

· 책임 추적 가능(Accountability)

현재 콘텐츠들을 일일이 수작업으로 모니터링 한다고 하지만 현실적으로 하나하나 모두를 확인할 수는 없었고, 명확한 책임이 따르지 않았다. 하지만 TDCDA에서는 관리자가 키 값을 이용하여 확인을 해야만 콘텐츠가 최종 업로드 되어 이용할 수 있게 되므로 관리자는 사전에 꼭 한번은 검증을 해야 한다는 관리자의 명확한 역할이 생기게 된다. 또한 최초 확인 시 로그 기록이 남게 되므로 향후에 발생할 수도 있는 사건·사고에 대비하여 관리자에게 문제가 된 콘텐츠의 유포 책임의 추적이 가능하다.

· 불법 콘텐츠 배포의 사전 방지

콘텐츠 업로드는 신분 확인을 거친 사용자만이 가능하므로 콘텐츠 제공자의 신뢰성이 보장된다. 또한 사용자 등록 시 할당된 공개키를 이용하여 암호화된 동영상을 업로드 하게 되며 관리자는 키 값을 이용하여 콘텐츠를 검증한 후에, 인증된 콘텐츠만이 최종 업로드 되므로 불법·유해 콘텐츠의 유통을 사전에 미리 막을 수 있다.

· 저작권(Copyright) 보호의 용이성

검증된 콘텐츠에 DRM 기술을 적용함으로써 배포자의 저작권을 보장하고 콘텐츠의 무단 복제를 방지할 수 있다. 또한 사용자 신분 확인 후, 속성 인증서의 부가정보에 기록된 정보로 콘텐츠의 출처와 원 저작자 등의, 저작권 관련 정보를 자동적으로 확인 할 수 있다. 이는 관리자가 일일이 확인하지 않아도 되므로 저작권 관리가 용이해질 뿐 아니라 사후 문제발생시 명확히 증명되어 질수 있다.

Ⅵ. 결론 및 향후 연구 방안

디지털 콘텐츠는 새로운 마케팅의 한 수단으로 지금도 많은 성공 사례를 낳고 있으며, 모바일 환경과 IPTV 등 통방 융합 환경 속에서 더욱 성장하게 될 것이다. 이러한 디지털 콘텐츠의 지속적인 성장이 가능하기 위해서는 불법 디지털 콘텐츠의 유통, 저작권 문제 등의 단점을 해결하여야 할 것이다. 본 논문에서는 콘텐츠 배포 시 신뢰성 확보, 콘텐츠의 무결성 및 저작권 보호 메커니즘을 통한 신뢰할 수 있는 콘텐츠 유통 방안 TDCDA(Trusted Content Distribution Architecture)를 제시하였다.

디지털 콘텐츠의 효과적인 보호를 위해서는 콘텐츠의 제작에서 배포, 활용까지의 전 과정에 걸친 보호 메커니즘의 제시가 필요하며 실제 정보보호 기술과의 연동을 통한 안정성 확보가 좀 더 필요한 부분이라고 생각된다. 향후 현업에서 활용가능 한 현실적인 타겟(예: CP, ISP, IPTV 등)을 제시함으로서 실효성을 높일 수 있는 연구를 진행할 예정이다.

참고문헌

[1] 박지현, 정연정, 윤기송, “DRM 기술 동향”, 한국전자통신연구원, 전자통신동향분석 제 22권 제4호, 2007.

[2] 최동진, “2007년도 국내 디지털콘텐츠산업 시장조사 보고서”, 한국소프트웨어진흥원, 2008.

[3] 오원근, “DRM 표준화 및 평가 기술”, 한국전자통신연구원, 전자통신동향분석 제20권 제4호, 2005. pp. 71-79, May 1997.

[4] 강호갑, “DRM 최신 국제표준 기술사양 분석 및 세계유명제품 동향과 전망에 관한 연구”, 한국소프트웨어진흥원, 2004.

[5] Danny Bradbury, “Decoding digital rights management”, Computer& Security, Vol. 26, Feb. 2007.

[6] 디지털 저작권 보호 기술, http://222.kisi.or. kr/information/information_list.asp, 한국표준협회.

[7] Santa Argeste, Guido Andaloro, Daniela Prestipino, and Lugia Puccio, “An image adaptive, wavelet-based watermarking of digital images”, Journal of Computational and Applied Mathematics, In Press, Corrected Proof, Available online 1, Feb. 2007.

[8] Hyun-Jun Choi, “Digital watermarking technique for holography interface patterns in a transform domail”, Optics and Lasers in Engineering 46(2008) pp. 343-348, 2008.

[9] 윤재석, 이재일, “아프리카 주요국가 공개키 기반 구조(PKI) 구축 현황 및 시사점”, 정보통신연구진흥원, 2005.

[10] Bogdan Ksiezopolski, Zbigniew Kotulski, “Adaptable security mechanism for dynamic environments:, Computers & Security, In Press, Corrected Proof, Available online 14, Dec. 2006.

[11] 김영철 외, “멀티미디어 정보보호 : Web 환경에서 컨텐츠 보호를 위한 PMI 기반의 해킹방지 eDBMS”, 한국멀티미디어학회, 멀티미디어학회논문지, 8권, 5호, 2005.

[12] David W. Chadwick, “An X.509 Role-based Privilege Management Infrastructure”, Business Briefings : Global InfoSecurity, World Markets Research Centre, 2002.

<著者紹介>

홍 승 필 (Seng-phil Hong) 종신회원
1993년 : Indiana State University (학사)
1994년 : Ball State University (석사)
1997년 : Illinois Institute of Technology (박사수료)
2003년 : 한국정보통신대학교 (박사)
1997년~2004년 : LG CNS System, Inc.
2005년~현재 : 성신여자대학교 미디어정보학부
<관심분야> 접근제어, 통합인증, 정보보호 아키텍처, 유비쿼터스 보안, 프라이버시 보호

김 혜 리 (Hye-ri Kim) 학생회원
2007년 : 성신여자대학교 미디어정보학부 졸업(학사)
2007년~현재 : 성신여자대학교 대학원 전산학과 (석사)
<관심분야> 개인정보보호

이 철 수 (Lee ChulSoo) 정회원
1977년 : KAIST 전산과 석사
1981년 : KAIST 전산과 박사
1982년~1993년 : (주)데이콤
1993년~1998년 : 한국전산원
1999년~2000년 : 한국정보보호원
2000년~2002년 : 정보통신대학교
2003년~현재 : 경원대학교 IT대학
<관심분야> 정보보호 정책, 침해사고 대응기술