디지털산업정보학회 논문지 제6권 제2호-2010년 6월

네트워크 서비스 환경에서 MPEG-21을 활용한 디지털 콘텐츠 보호 및 컴퓨터 포렌식스 증거 관리 메커니즘

장 은 겸* · 이 범 석**

Digital Content Protection and Computer Forensics Evidence Management Mechanism using MPEG-21 in Network Service Environment

Jang, Eun Gyeom · Lee, Bum Suk

〈Abstract〉

In network service environment, cultures from diversified fields are easily accessible thanks to the convenient digital content services. Unfortunately, unauthorized access and indiscreet misuse behaviors have deprived content owners of their copyrights. This study suggests an integrity-ensured model applicable for forensic evidence of digital content infringement in network service environment. The suggested model is based on MPEG-21 core components for digital content protection and the system is designed in connection with the components of digital content forensics.

Also, the present study suggests an efficient technology to protect and manage computer forensic evidence and digital content by authorizing digital content use and catching infringing logs of authorized users without lag in network environment for the benefit of network security and reliability.

Key Words : Computer Forensics, Digital Copyrights Management, Network Service, MPEG-21, Evidence Management

Ⅰ. 서론

오늘날 유·무선 통신망을 이용한 네트워크 서비스는 다양한 문화를 빠르고 쉽게 접할 수 있도록 한다. 이러한 서비스의 일환으로 RFID(Radio- Frequency IDentification)의 기술을 활용한 유비쿼터스 및 홈 네트워크 환경을 제공하고 있다. 이것은 초고속 인터넷 서비스 및 실시간 멀티미디어 서비스 환경에서 댁내 자원의 공유, 네트워크를 이용한 오락, 교육, 진료 및 홈 쇼핑 등 각종 부가서비스, 휴대 정보단말기를 이용한 원격 자동제어, 홈 보안 기능 등을 제공한다[1].

이러한 네트워크 서비스 환경의 발전에 힘입어 많은

* 대전대학교 컴퓨터공학과 겸임교수(제1저자)
** 혜천대 유아교육과 교수(교신저자)

콘텐츠가 대내·외로 유통되고 있다. 그러나 디지털 콘텐츠는 아날로그 콘텐츠와는 달리 무한대의 복제가 가능할 뿐만 아니라 인터넷을 통해 전세계 어디라도 순식간에 전파될 수 있는 특성을 지니고 있기 때문에 불법복제로 인한 폐해가 사회적 이슈로 제기되고 있다. 이러한 디지털 콘텐츠의 불법복제를 방지하기 위해 DRM(Digital Rights Management)기술이 등장하였다. 그러나 DRM은 콘텐츠의 사용권한을 관리하기 위한 기술이므로, 비인가된 사용에 대한 대응방안이 미흡하다.

본 논문에서는 네트워크 서비스 환경에서 비인가된 사용자의 콘텐츠 오용행위 및 접근에 대응하기 위해 전자적 증거 수집 및 관리를 지원하는 디지털 콘텐츠 보호 모델을 제안한다. 본 제안논문은 기존의 컴퓨터 포렌식스 기술을 이용하며, 컴퓨터 포렌식스의 요구조건인 절차적 증거수집으로 신뢰증거를 확보한다. 또한, MPEG-21의 핵심사항을 기반으로 디지털 콘텐츠를 보호하였다. 즉, 네트워크 기기에서 디지털 콘텐츠의 불법적 오용 및 침해증거를 안전하게 관리하여 포렌식스 정보로 활용할 수 있도록 하였다.

Ⅱ. 컴퓨터 포렌식스

2.1 컴퓨터 포렌식스 연구 동향

컴퓨터 포렌식스를 위한 관련 연구기관은 대표적으로 미국 법무부, CFTT(Conputer Forensics Tool Testing), HTCN(High-Tech Crime Network), CERIAS(Center for Education and Research in Information Assurance and Security), ASCLD(American Society of Crime Laboratory Directors), IACIS(the International Association of Computer Investigation Specialists)를 들 수 있다.

미국 법무부는 전자증거물에 대한 압수 수색 절차를 안내하는 가이드라인을 발행하고 CCIPS(Computer Crime and Property Section)를 개설하여 컴퓨터 범죄에 관련된 문서들을 비롯해 주요 인프라 보호 요령, 지적재산권 보호, 전자상거래의 법적 문제에 관한 세션들을 담고 있다. CFTT는 포렌식스 도구가 필수적으로 갖추어야할 기능에 대한 요구사항을 목록화하고 그 기능을 잘 수행하는지에 대해 평가할 수 있도록 포렌식스 소프트웨어 도구를 평가할 수 있는 방법론을 제시하고 있고 HTCN는 컴퓨터 포렌식스에 관련된 교육 및 테스팅 기관 정보, 컨퍼런스, 세미나 등 교육정보, 컴퓨터 포렌식스 관련 도구 및 기술 자료들에 정보를 제공하고 있다.

또한 CERIAS와 ASCLD에서는 기술적인 내용에 대한 연구뿐만 아니라, 교육, 법분야, 언어분야, 경제분야 문제들에 대한 관계와 그 의존성에 대한 연구를 병행하고 연구시설이나 기관들이 컴퓨터 포렌식스를 수행함에 있어서 따라야 할 기준을 제정하여, 이러한 사항들을 이행할 것을 요구하고 있다.

이 밖에도 Proficiency Testing 및 지속적인 교육과 트레이닝 활동을 규정해 놓고 있다. 그리고 IACIS에서는 컴퓨터 범죄 처리 절차를 만들어 컴퓨터를 압수하고 컴퓨터에서 전자적 증거물을 획득하는 방법을 확립했으며 교육과정을 설립해 포렌식스 전문가를 위한 지속적인 훈련을 진행하고 있다[2].

2.2 컴퓨터 포렌식스 도구 분석

2.2.1 EnCase

EnCase[3]는 많은 양의 컴퓨터 증거를 쉽게 관리하고 파일 스택과 할당되지 않은 데이터를 볼 수 있는 GUI의 특징을 가지고 미 연방 법원의 EnCase를 통해 얻은 결과물을 법적인 증거로 채택한 판례로 더욱 성능을 인정받고 있는 도구이다.

Encase는 윈도우(NTFS, FAT 16/32), 리눅스(ext2), 유닉스(UFS), MacOS 파일 시스템 분석 기능과 증거 자료로서의 무결성을 보장하기 위해서 피해 시스템의 하드

디스크를 MD5 hash algori템의m을 사용하여 digi템hasfinger printing의 증거자료의 무결성 보장몸결성gi템hasfinger printing)한다. 또한 다양한 이미지 추출 방법을 제공한다.

2.2.2 TCT

TCT(The Coroner's Toolkit)[4-5]은 침해 사고 발생 당시의 이벤트 수집 및 분석을 보다 정확하고 수월하게 수행하기 위한 기능을 제공한다. 피해 시스템의 상태 정보에 대한 snapshot을 생성하며, 백업된 디스크 이미지 분석 및 파일 복구에 유용하게 사용할 수 있다.

TCT 구성 프로그램의 주요 기능은 피해 시스템의 휘발성 정보를 캡쳐한다. 네트워크 상태 정보, 주요 설정 파일, 일반 시스템 정보, 메모리에 로그된 프로세스, 파일시스템의 inode 정보를 수집, 기본적으로 지워진 파일에 대한 inode 정보를 제공, 다양한 옵션을 사용하여 inode에 대한 정보를 수집한다. 또한 복구된 파일의 file type를 출력하고 파일시스템에서 할당되지 않은 디스크의 블록들을 분석하고 복구, 파일의 접근, 수정 시간을 조사하고 timeline 생성한다.

2.2.3 기타 도구

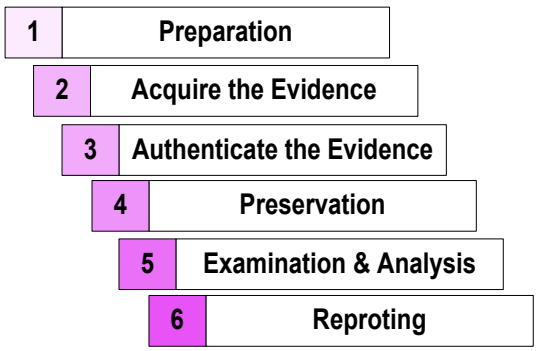
TCTUtil, Sleuth Kit, Autopy forensics Browser은 TCT 프로그램과 유사한 기능을 갖추고 있다. Sleuth Kit는 NTFS, FAT, FFS, EXT2FS, EXT3FS를 지원해 다양한 파일 시스템을 분석할 수 있다. 또한 Autospy는 피해 시스템 분석을 진행하는데 있어서 작업을 용이하게 하기 위해 개발된 웹 브라우저 기반의 GUI 프로그램이다[6-7].

EScript(스크립트 검색 도구)를 이용하여 숨겨진 E-Mail, NT Security event log, Internet History 등을 검색하고, 일반 텍스트와 HTML 형식을 지원하는 레포팅 기능과 삭제된 파일과 비할당 클러스터 영역 검색 및 복구 기능을 제공한다.

2.3 컴퓨터 포렌식스 절차

컴퓨터 포렌식스 처리 절차는 세 가지 단계로 구성되는데, 첫 번째는 증거물 확보 단계로 본래의 디지털 정보를 변경하거나 손상이 없이 증거물을 확보하고 두 번째는 증거물 인증 단계로 증거물의 본래의 현물에서 획득한 데이터와 동일함을 인증하며 세 번째는 증거물 분석 단계로 증거물의 변형 없이 분석을 수행한다.

모든 사건의 경우 기본적으로 위의 3단계를 준수하여야 하며, 구체적인 절차의 명세는 주어진 환경과 목적에 따라 달라진다[8]. Warren G는 Incident Response Essential에서 기본 3단계의 포렌식스 절차를 그림 1과 같이 6단계로 확장 하였다.



<그림 1> 컴퓨터 포렌식스 절차

증거물 획득 단계에서는 침입행위인 디지털증거, 휘발성 증거를 수집하며, 하드 디스크를 이미징한다. 증거물 인증 단계에서는 증거물의 전송에 있어서 데이터의 무결성을 검증한다. 또한, 증거물의 보관 및 이송 단계에서는 디스크를 물리적으로 통제하며, 증거물 분석 단계에서는 파일분석, 암호제거, 슬랙 영역 분석 등을 수행한다.

2.4 기존 연구 및 환경에서의 문제점

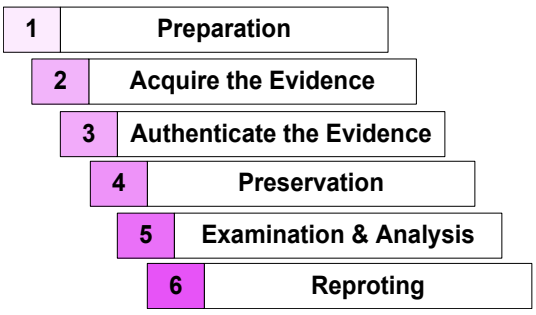
현재 침해 증거를 확보하기 위한 환경 및 기술은 오프

라인상에서 증거물이 확보되고 있다. 또한 네트워크 환경에서 증거수집 에이전트를 통해 증거물을 수집하고 관리하는 기술이 연구되고 있다. 그러나 증거 데이터의 양이 방대하여 네트워크 트래픽을 발생하고 있으며, 네트워크 환경에서의 안전성을 보장하지 못한다. 이러한 문제점을 보완하고자 증거물 관리에 네트워크 트래픽을 줄이고 네트워크 영역에서 증거물의 신뢰성을 보장하기 위한 기술을 본 논문에서 제안한다.

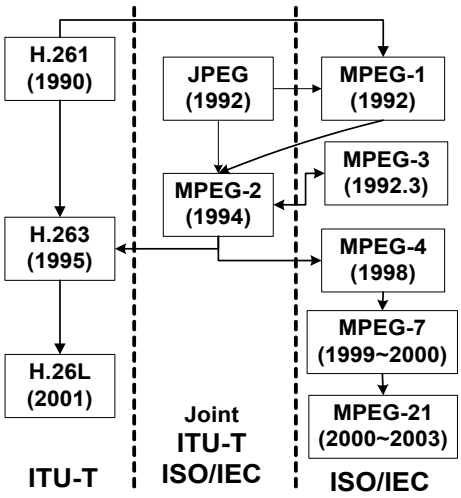
Ⅲ. MPEG-21 기술

3.1 멀티미디어 표준 MPEG

MPEG(Motion Picture Experts Group)은 국제 표준화 기구(International Organization for Standardization: ISO)와 국제 전기 위원회(International Electrotechnical Commission: IEC)가 정보 표현의 표준화를 위해 구성한 공동기술위원회(Joint Techni -cal Committee1: JTC1) 산하 전문부회(Sub-Committee 29: SC29)의 별칭으로 동영상과 오디오의 압축 및 다중화에 관한 표준을 제정하여 왔다. 현재까지 진행된 표준은 그림 2[9]와 같이 MPEG-1, MPEG-2, MPEG-3, MPEG-4, MPEG-7, MPEG-21이 있다.



<그림 1> 컴퓨터 포렌식스 절차



<그림 2> MPEG 표준화 현황

멀티미디어 표준은 ISO/IEC 뿐 아니라 다른 기관에서도 추진하고 있으며, ITU-T에서 제정한 표준은 미디어 압축과 관련된 표준인 H.261, 압축 및 처리에 관련된 표준인 H.263, MPEG-21과 같이 멀티미디어 프레임워크 표준인 H.26L이 있다[10].

3.2 MPEG-21 멀티미디어 프레임워크 구성

MPEG-21[10] 멀티미디어 프레임워크는 멀티미디어 비즈니스 모델과 밀접하게 관련하여 다음과 같은 일곱 가지 요소 기술들로 정의된다[11].

① Digital Item Declaration
② Digital Item Identification and Description
③ Content Handing and Usage
④ Intellectual Property Management and Protection
⑤ Terminals and Networks
⑥ Content Representation
⑦ Event reporting

3.2.1 Digital Item Declaration

가장 기본적인 기술 중의 하나인 디지털 아이템 정의 모델은 체계적이고 융통성이 있으며 상호호환적인 스키마(schema)에 관한 것이다.

이 모델은 사용자가 이용하는 터미널이나 네트워크에 적절하게 이용하고자 하는 디지털 아이템으로 구성이 가능한(configurable) 요소를 제공한다. 정의된 디지털 아이템은 크게 컨테이너와 아이템이라는 디지털 아이템 요소로 구분되어져 있다. 컨테이너는 아이템들이 패키지된 형태이고, 아이템은 하위 레벨의 아이템이나 혹은 멀티미디어 콘텐츠의 부품과 같은 컴포넌트(component)에 의해 정의된다. 그 중 아이템은 이 아이템을 사용자의 요구 조건(해상도, 포맷 등)에 맞게 구성할 수 있는 요소인 CHOICE와 SELECTION에 의해 configuration될 수 있다.

3.2.2 Digital Item Identification and Description

디지털 아이템의 속성, 타입이나 구조적 형태와 관계없이 그 객체들을 식별, 묘사할 수 있는 표준적 프레임워크에 관한 것이다.

오늘날 표준화 기술들은 특정 미디어 타입에 응용될 수 있는 콘텐츠 식별 및 묘사에 관한 메타데이터 프레임워크로서 MPEG-21 환경 하에서의 다양한 멀티미디어 타입에 대해서 통합적으로 응용하기 힘든 문제를 가지고 있다.

이러한 문제를 해결하기 위하여 MPEG-21에서는 unique, persistent, reliable, accurate, seamless ID 시스템과 디지털 아이템 검색 에이전트의 자동 검색, retrieval, acquisition이 가능하게 하기 위한 integral, integrated description system 표준화 작업을 제안, 연구하고 있다.

3.2.3 Content Handling and Usage

User(s)가 원하는 디지털 아이템을 제공하기 위한 interaction model에 관한 표준화 기술이다.

콘텐츠의 전송 및 이용은 사전에 미리 정해진 네트워크와 터미널을 통하여 이루어지고 있으며 어떤 임의의 네트워크와 터미널을 통한 User들간의 자유로운 콘텐츠 전송 및 이용은 어렵다. 따라서 분산 환경 하에서의 표준화된 저장 및 관리 기법이 요구된다.

이러한 문제점을 해결하기 위하여 다음과 같은 네 가지 표준화를 위한 요구 조건이 있다. 첫째, 콘텐츠와 묘사에 대한 검색, 저장, 이용에 관한 표준화, 둘째 소비자에 관한 profile handling에 관해서 프라이버시를 제어와 사용자가 자신의 선호도를 표현할 수 있는 표준화된 기법의 포맷 표준화, 셋째 User가 원하는 콘텐츠 구성에 관해서 사용자의 개인 성향 혹은 선호도에 따른 자동화된 구성/재구성 기법을 표준화, 넷째 프레임워크 내에서 지능 에이전트를 이용할 수 있는 인터페이스와 프로토콜을 정의이다.

3.2.4 IPMP

IPMP(Intellectual Property Management and Protection)는 지적 재산으로서 가치 있는 콘텐츠들을 영속적으로 유지 관리하며, 이를 거래시 신뢰할 수 있는 관리 및 보호 방법에 관한 표준화 요소 기술이다

디지털 아이템에 대한 관리 및 보호 방법에 IPMP 시스템의 상호호환성과 정보보호를 위한 기술이 부족하다. 이러한 문제를 해결하기 위해 MPEG-21 IPMP 요소 기술에서는 “IPMP를 위한 추가적인 하드웨어를 최소화”, “User들 간의 의사 소통이 가능한 표준기술제공”, “사용자의 개인정보보호”, “콘텐츠와 보유 사용자의 권한 유지”, “콘텐츠 권리 취득 및 양도”, “연속적인 보안과 보안의 갱신”, “ 콘텐츠의 가치에 따라 관리 및 보호의 비용 고려”, “ IPMP 시스템은 현제 가용한 기술로 구현 가능”등을 포함한다.

3.2.5 Terminals and Networks

다양한 네트워크와 터미널 하에서 콘텐츠가 상호호환

적이고 투명하게 접근 이용될 수 있는 기술의 표준화 기술이다.

네트워크와 터미널의 기술적, 관리적 사양과 관계없이 End-User가 디지털 아이템을 상호호환적이고 QoS에 맞는 이용을 가능하게 하기 위하여 "터미널 QoS 관리를 위한 API와 관련된 Protocol의 표준화", "네트워크 QoS 관리를 위한 NPI(Network Program Interface)와 관련된 Protocol의 표준화", "터미널과 네트워크 공용의 QoS 관리를 위한 API와 관련된 Protocol의 표준화"작업을 진행한다.

3.2.6 Content Representation

미디어 자원을 효율적으로 표현할 수 있는 표준적 기술을 제공한다.

멀티미디어 프레임워크에서 콘텐츠는 전송 효율을 높이기 위해 압축된다. 그리고 손쉽게 검색 또는 관리하기 위하여 식별자(ID)가 부여된다. 전송된 콘텐츠 내용에 어떠한 내용이 포함되었는지 알기 위하여, 디지털 아이템 묘사와 같은 기술이 이용된다. 이러한 메타데이터와 함께 콘텐츠 내용이 전송, 저장, 보호, 거래 및 소비가 이루어진다. MPEG-21에서는 디지털 아이템이라는 콘텐츠에 AV뿐만 아니라 디지털 아이템 식별자와 묘사와 같은 메타데이터를 포함한다[11].

현재 표준화되어 있는 콘텐츠의 코딩 혹은 포맷으로 정지화상의 경우, JPEG, JPEG-LS, JPEG 2000, GIF 등이 있다. 동영상의 경우, 프레임 기반의 H261, H263, MPEG-1/2 Video 그리고 객체 기반의 MPEG-4 Visual 등이 있다. 오디오와 관련된 표준으로 MPEG-1/2/4 Audio 등이 있다. Synthetic AV의 경우, VRML, MPEG-4 AV 및 MIDI와 같은 표준이 있다. 기존의 개발된 혹은 개발 중인 표준들은 다양한 멀티미디어 타입들을 이용하는 MPEG-21 환경에서 Content Representation 요소 기술에 대해 단편적인 접근 방법을 제공한다.

3.2.7 Event Reporting

모든 User들간 혹은 User와 디지털 아이템간에 발생하는 모든 상호작용의 항목, 내용 등을 어떻게 표준적으로 정의할 것인가에 관한 기술이다.

일종의 Post-Processing 과정으로서 디지털 아이템의 생성부터 이용과 관련된 모든 사건을 정확하게 모니터링함으로서 이와 관련된 처리과정을 효율적이고 최적화하기 위한 목적을 가지고 있다. Financial, Network Service Delivery, Advertising 분야 등에서 지적재산권과 관련된 디지털 아이템이 다루어지고 있는 것으로 알려졌지만, 통합적이고 표준적이며 상호호환적인 Event Reporting metrics와 interface가 없는 것이 사실이다.

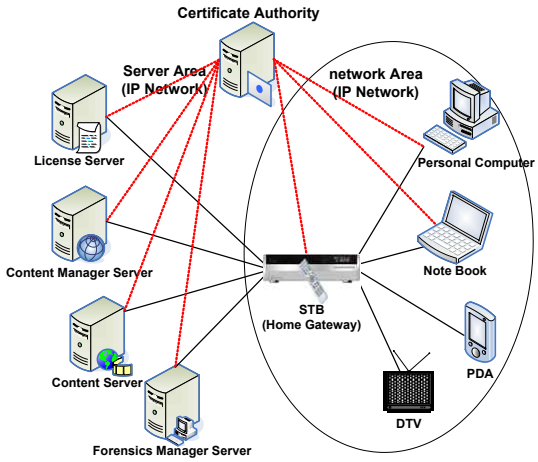
현재 MPEG-21에서는 디지털 아이템 선언, 디지털 아이템 식별 및 기술, 콘텐츠 취급 및 사용, 콘텐츠 표현, 지적재산권 관리 및 보호, 터미널 및 네트웍, 이벤트 리포팅 등의 7가지 기본 기술요소를 설정하고 각 요소 기술에 대한 세부 표준을 제시하고 있다[10-11].

Ⅳ. 디지털 콘텐츠 보호 메커니즘

4.1 시스템 개요

본 논문의 제안 모델의 시스템 구성은 그림 3과 같이 서버 영역, 네트워크 영역, 인증 영역으로 분류된다.

라이센스 서버는 LMS(License Management Server), LIS(License Issuing Server)가 존재하며, 이중 LMS는 라이센스의 생성, 제거, 권한 부여 등 라이센스 전체적 메커니즘을 관리하고, LIS는 라이센스의 LMS에서 생성한 라이센스를 발급한다. 콘텐츠 관리 서버는 콘텐츠의 메타데이터, 콘텐츠ID, 콘텐츠 암호화키 등 콘텐츠 보호에 관련된 정보를 관리한다. 콘텐츠 서버는 디지털 콘텐츠를 VOD형식 또는 유니케스팅 방식으로 서비스를 제공하고, 이때 전송되는 디지털 콘텐츠는 기밀성이 보호되



<그림 2> 시스템 구성

어야 한다. 포렌식스 관리 서버는 네트워크 영역의 각 장치에 전송되는 증거데이터의 무결성을 보장하며, 저장·관리 기능과 각 클라이언트의 증거 데이터 전송을 통제한다.

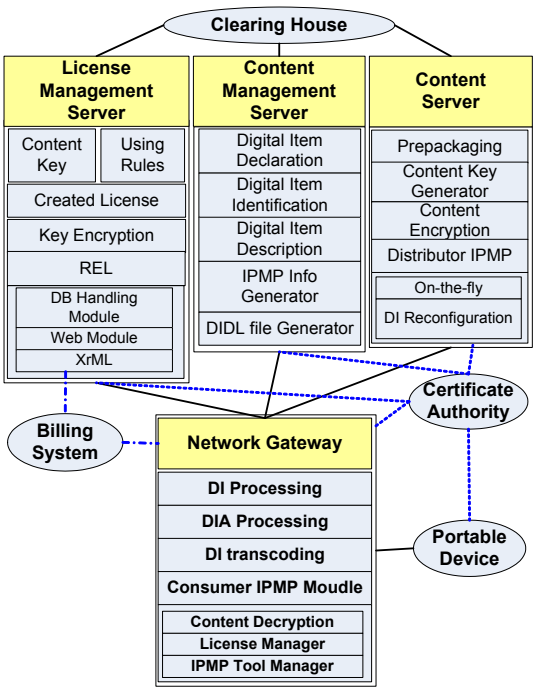
STB(Set-Top Box)는 서비스 게이트웨이 역할을 수행하며, PC(Personal Computer), 노트북, PDA, DTV등을 외부 네트워크와 연결한다. 네트워크 영역의 모든 장치들은 포렌식스 에이전트를 포함하며 서버 영역의 모든 기기들과 네트워크 영역의 모든 장치들은 CA(Certificate Authority) 서버에 연결되어 인증을 받을 수 있으며, IP 통신이 불가능한 기기들은 STB를 통하여 인증 받는다.

4.2 제안 모델 구성 요소

4.2.1 DRM 구성

정보와 서비스에 대한 접근은 터미널과 네트워크를 통해 시간이나 장소에 제약이 없다. 그러나 모델과 규칙·절차, 이해관계, 콘텐츠 포맷 등이 다양하여 커뮤니티들이 효과적으로 상호 작용하기란 현실적으로 불가능하다. MPEG-21 멀티미디어 프레임워크는 이렇게 상이한 커뮤니티들이 서로 협동적으로 구성 될 수 있도록 하는 것이며, 서로 다른 모델, 규칙, 절차, 콘텐츠 포맷의 구현과 통합을 보조하는 것을 목표로 한다. 이에 본 제안 모델의 DRM 구성은 MPEG-21의 프레임워크를 따르며, 콘텐츠 식별, 표현, 관리, 보호를 중심으로 모듈의 구성은 그림 4와 같다.

LMS은 콘텐츠 키, 사용규칙, 라이센스 생성, 콘텐츠 보호키 암호화, REL관련 요소로 구성되고, CMS는 DID, DII, IPMP info요소로 구성된다. 또한 CS(Content Server)는 패키져, 콘텐츠 보호키 생성, 콘텐츠 암호화, IPMP 모듈 등으로 구성, STB는 DI, DIA 프로세서와 IPMP 모듈로 구성된다.



<그림 4> DRM 구성

DRM 모든 구성요소들은 CA에 의해 인증되고, LMS는 라이센스 생성시 사용자의 공개키를 취득한다. 또한,

모든 서버는 공통 데이터를 클리어링 하우스를 통해 공유되며, LMS와 네트워크 게이트웨이는 빌링 시스템과 연동된다.

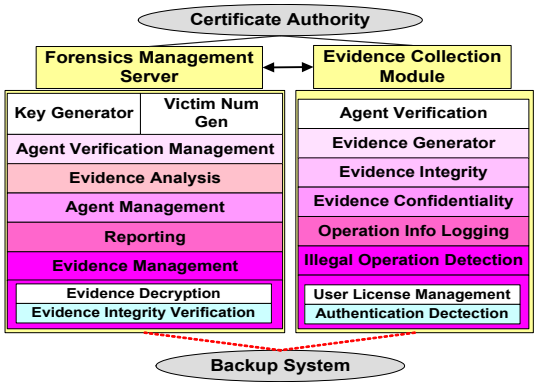
4.2.2 디지털 콘텐츠 포렌식스 구성

컴퓨터 포렌식스에서 디지털 증거의 획득, 분석, 보존에 주체인 기록은 생성한 프로그램의 신뢰성이 입증되어야 증거로 사용할 수 있다. 그러므로 컴퓨터 포렌식스는 일정한 절차에 따라 수행 되어야 한다.

그림 1의 컴퓨터 포렌식스 절차 중 증거 수집은 2, 3 단계로 증거 수집과 증거 인증을 수행하며, 네트워크 영역의 기기에서 실행된다. 증거 관리 모듈은 4, 5, 6단계로서 증거물의 보관, 분석 레포팅을 수행하며, 포렌식스 관리 서버에서 수행 된다. 디지털 콘텐츠 포렌식스를 위한 구성(그림 5)의 증거 수집 모듈의 세부기능은 다음과 같다.

- 첫 번째, 에이전트는 증거물에 접촉하는 모듈로서 제3의 공인된 기관에 의해서 검증 받은 에이전트이다.
- 두 번째, 증거 수집 모듈의 기능은 시스템의 침해 증거의 로그를 수집하며, 이때 증거의 무결성과 기밀성이 보장되어야 한다. 이와 함께 증거물의 수집 활동이 정당한 절차에 의해서 이행되었음을 검증하기 위한 활동정보를 로깅 한다.
- 마지막으로 증거 수집 모듈의 핵심 기능으로서 비정상 행위를 탐지한다. 비정상 행위는 라이센스의 비정상적인 활용이나 변경 등을 의미하며, 인가되지 않은 사용자의 콘텐츠 접근 등이 있다.

그림 6은 MPEG-21의 REL중 재생 권한 라이센스의 캡쳐 화면이다. 증거 수집 모듈은 그림 6과 같은 라이센스 예제파일에서 라이센스의 메시지 다이제스트 엘리먼트를 추가하여 재생 종료와 같은 라이센스 변경사항 발생시 라이센스를 업데이트한다.

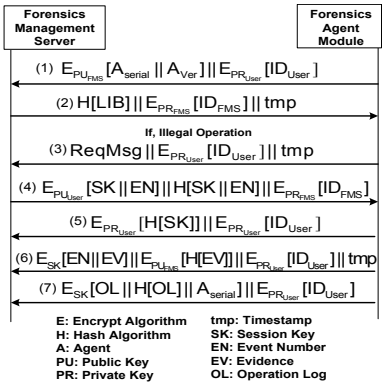


<그림 5> 디지털 콘텐츠 포렌식스 구성

<그림 6> 라이센스 예제 파일

이와 함께 서버에 변경된 라이센스 다이제스트 값을 전송하여 추후 비정상 행위 탐지에 사용하게 된다. 또한 라이센스 증거 데이터 전송시 기존의 컴퓨터 포렌식스 시스템에서는 증거 데이터 전부 또는 디스크 이미지를 전송하나, 제안모델에서는 라이센스 중 사용권한과 관련된 엘리먼트인 그림 6의 블록 부분만 전송 가능하므로 네트워크 자원의 이용과 증거 데이터의 암·복호화 시간을 최소화 한다.

증거 전송시 증거 데이터의 무결성과 기밀성을 보장하며, 출처 인증 등의 보안 서비스 제공을 위한 전송 메커니즘은 그림 7과 같다.



<그림 7> 증거 전송 메커니즘

포렌식스 에이전트와 포렌식스 관리 서버는 관용화 암호 알고리즘(AES/DES)과 공개키 암호 알고리즘을 이용하여 정보를 암호화하고 PKI 기반의 X.509인증서와 PEM형식 파일을 이용하여 키를 분배한다.

포렌식스 에이전트 모듈은 실행과 동시에 현재 모듈의 무결성 검증을 위해 시리얼 번호와 버전 정보를 서버에 전송한다.

(1) $E_{PU_{FMS}}[A_{serial} \| A_{Ver}] \| E_{PR_{User}}[ID_{User}]$

이때, 출처인증을 위해 자신의 ID를 개인키로 암호화하여 전송한다. 서버는 에이전트의 버전 정보를 기반으로 라이브러리의 MAC (Message Authentication Code)를 생성하여 TT(Time sTamp)와 함께 전송한다. 서버 또한 자신의 출처 인증을 위해 FMS(Forensics Management Server)의 ID를 개인키로 암호화하여 전송한다.

(2) $H[LIB] \| E_{PR_{FMS}}[ID_{FMS}] \| tmp$

클라이언트가 불법적인 행위를 탐지할 경우 에이전트 모듈은 서버에 증거를 암호화할 세션키를 요구하고, 서버는 이에 대한응답으로 세션키와 사건 번호를 사용자의 공개키로 암호화하여 전송한다.

(3) $ReqMsg \| E_{PR_{User}}[ID_{User}] \| tmp$

(4) $E_{PU_{User}}[SK \| EN] \| H[SK \| EN] \| E_{PR_{FMS}}[ID_{FMS}]$

에이전트는 서버에서 전송한 세션키로 증거와 사건번호를 암호화하고 증거의 무결성 보장을 위해 증거의 해쉬 코드 값을 계산하여 함께 전송하며, 사건 발생 시간을 저장하기 위해 TT를 함께 전송한다. 또한, 정당한 절차에 의해 증거가 생성됐음을 증명하기 위해 에이전트 활동정보를 FMS에 전송한다.

(5) $E_{PR_{User}}[H[SK]] \| E_{PR_{User}}[ID_{User}]$

(6) $E_{sk}[EN \| EV] \| E_{PU_{FMS}}[H[EV]] \| E_{PR_{User}}[ID_{User}] \| tmp$

(7) $E_{SK}[OL \| H[OL] \| A_{serial}] \| E_{PR_{User}}[ID_{User}]$

FMS는 그림 5와 같이 증거 기밀성 보장을 위한 키 생성, 피해시스템 번호 생성, 에이전트 검증, 증거 분석, 에이전트관리, 레포팅, 증거 관리를 지원한다. 증거 관리를 위해 복호화, 증거 무결성 검증과 증거 분석시 시간 또는 연관데이터 분석이 가능해야 한다. 그림 8은 증거 분석을 위해 포렌식스 관리 시스템에 전송된 데이터이다.

```
- <keyHolder>
  - <info>
      <dsig:KeyName>AES-CBC-256</dsig:KeyName>
    </info>
  </keyHolder>
- <allConditions>
  - <sx:exerciseLimit>
      <sx:count>4</sx:count>
    </sx:exerciseLimit>
  - <sx:feeFlat>
    - <sx:rate>
        <sx:amount>2000</sx:amount>
        <sx:currency>IUY</sx:currency>
      </sx:rate>
    </sx:feeFlat>
  </allConditions>
</grant>
- <issuer>
  - <keyHolder>
    - <info>
        <dsig:KeyName>Agent Number: AE57C003574
        </dsig:KeyName>
      </info>
    </keyHolder>
  </issuer>
- <evidence>
  - <integrity>
      <hash>3f9ec876181a3c170f1df94e6a038334c289
      20adf26b8e040d28198915e705a3</hash>
    </integrity>
  </evidence>
</license>
```

<그림 8> 증거 데이터와 무결성 값

V. 제안 모델 성능 평가

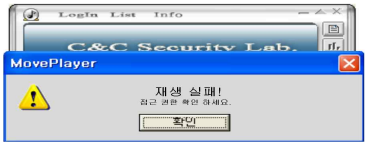
성능평가는 DRM 측면의 검증과 포렌식스 모듈 영역으로 구분하여 평가한다. DRM 측면은 그림 4에서 기술한 MPEG-21의 핵심요소의 지원 유·무를 통해 분석하며, 콘텐츠 포렌식스 모듈은 네트워크 영역에서 증거물의 안전성과 네트워크에 미치는 트래픽을 비교·분석한다.

5.1 Dcon-Pro 모델에 MPEG-21 적용

Dcon-Pro Player은 디지털 콘텐츠를 보호모델로서 사용자를 식별 및 인증하고 디지털 콘텐츠를 제어하는 기능을 갖는다. 콘텐츠 접근 제어는 사용자의 시스템 정보(CPU, Hard Disk, MAC)를 활용하여 통제하고 콘텐츠의 유효성을 검사하여 콘텐츠를 관리한다. 또한 Digital Item의 선언에 대한 유연성을 갖는 기본 폼, Digital Item의 Identifi -cation과 description, Content Handling & Usage, Terminals & Networks, Content Representation, Event Reporting을 지원하며, Digital Item에 대한 저작권 보호 기능을 갖는다.

제안 모델의 평가를 위해 네트워크 환경에서 디지털 콘텐츠를 사용자 에이전트에 제공하고 정당한 사용자가 접근을 시도했을 때와 정당하지 않은 사용자가 접근을 했을 때의 시나리오를 기반으로 테스트 하였다. 그림 9는 "Dcon-Pro Player"실행 화면이다.

<그림 9> Dcon-Pro 0.9 Player



<그림 10> Dcon-Pro 0.9 Player 이벤트

그림 10과 같이 콘텐츠의 유효성 검사는 사용기간이 적용된 콘텐츠 헤더 값을 이용하여 침해 이벤트를 발생시켰다.

증거 수집은 본 이벤트에서 시작되며 MPEG-21을 활용하여 DRM를 적용시키므로 표 1과 같은 결과를 얻을 수 있다.

<표 1> DRM 요소 평가

핵심요소	지원여부	내 용
IPMP	○	디지털 콘텐츠의 보호를 위해 암/복호화를 이용하며, 라이센스를 통해 콘텐츠 이용 제어
DID	○	CMS를 이용한 디지털 아이템 선언
DII	○	CMS를 이용한 디지털 아이템 식별코드 제공 및 기술
Content Handling	○	콘텐츠 서버와 LMS, CMS를 이용하여 디지털 콘텐츠 관리, 저장, 검색 지원
Networks	○	기존의 네트워크뿐만 아니라 홈 네트워크까지 확장
Representation	△	현재 영상, 음성 데이터는 지원하나 텍스트, 그래픽은 미흡
Reporting	○	기존의 사건보고 뿐만 아니라 컴퓨터 포렌식스까지 지원

○: 지원 △: 부분지원

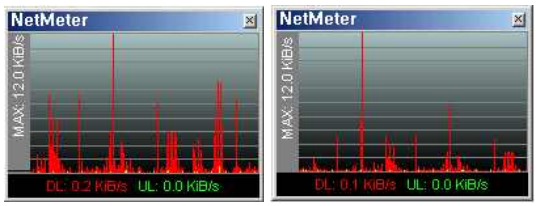
표 1의 결과는 MPEG-21 모델을 적용함으로서 제공되는 핵심 기능으로 포렌식스 증거 제공에 충분한 정보를 제공한다. 네트워크의 경우 현재 가장 보편적으로 사용하고 있는 WMRM의 경우, IP인터넷 망만을 지원하지만 본 모델은 네트워크 장치에서 공용으로 적용이 가능하다. 또한, 본 레포팅의 경우 기존의 라이센스 발급, 사용내역 저장뿐만 아니라 추후 저작권 침해 소송의 증거자료로 사용될 수 있도록 기밀성과 무결성이 보장된 신뢰된 정보를 생성할 수 있다.

5.2 Contents Forensics 요소 평가

콘텐츠 포렌식스 요소 평가는 기존의 컴퓨터 포렌식스 시스템과 본 논문에서 제안하는 모델의 네트워크 이용량

을 기반으로 평가한다. 기존의 컴퓨터 포렌식스 EnCase는 증거 수집시 디스크 드라이브를 전체 이미징 하거나 특정 폴더 또는 파일을 추출한다. 또한 생성된 파일들의 무결성을 검증하기 위해 새로운 파일을 생성한다. 그러나 본 모델은 기존의 라이센스 파일에 증거와 무결성 값을 추가한다. 라이센스는 콘텐츠 사용의 시작일, 사용기간, 운용횟수, 운용방식 등에 관한 권한을 규정하고. 콘텐츠 ID, 콘텐츠 복호키, 라이센스 인증서 등을 포함한다.

MPEG-21의 REL중 콘텐츠 재생권한 라이센스를 EnCase에 의해 증거를 수집하여 전송할 때는 우선적으로 라이센스 데이터의 크기는 2042 바이트와 무결성 검증에 SHA-256을 이용할 경우 64 바이트가 추가되어 2106 바이트가 된다. 그러나 제안 모델은 MPEG-21의 라이센스 관련 영역만을 추출한 968 바이트를 갖고 처리할 수 있다. 예를 들어, 콘텐츠 재생권한 라이센스의 증거가 1000일 때, Encase를 활용한 라이센스 파일 수집의 경우 평균 2136 바이트이며, MPEG-21의 라이센스를 활용하면 평균 72 바이트이다. 이와 같은 결과를 얻는 이유는 Encase에서는 라이센스에 관련한 파일과 폴더(DRM폴더: 윈도우 XP의 경우, C:\Documents and Settings\All Users\DRM)만을 추출하는 것이 아니라 디스크를 이미징하여 용량이 많아진다. 제안 모델에서는 MPEG-21에서 지원하는 라이센스 정보만을 수집하는데 차이가 있다. 그림 11은 네트워크 트래픽 모니터링 프로그램인 NetMeter 실행 화면이다.

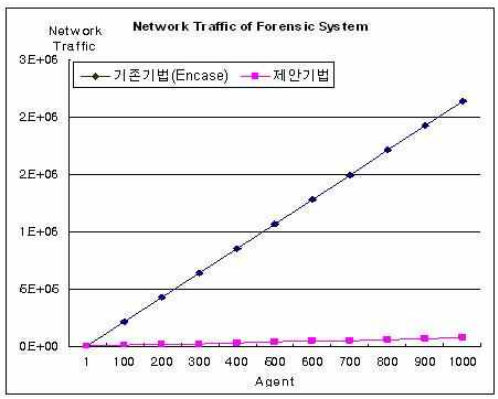


(a) Encase 증거전송 (b) 제안기법

<그림 11> 네트워크 트래픽

그림 11은 위의 결과를 바탕으로 포렌식스 관리시스템에 콘텐츠 재생권한 라이센스 증거만 전송될 경우 네트워크 트래픽을 나타낸 것이다. Encase에 의해 수집된 증거와 제안기법에서 수집한 증거를 임의의 주기로 포렌식스 서버에 전송할 때의 네트워크 트래픽 결과 이다. (b)의 경우, 일반적인 네트워크 트래픽과 비슷한 결과를 얻었고 (a)의 경우에는 트래픽의 차이를 식별할 수 있었다.

그림 11의 결과에 의해 에이전트 수를 증가한 시뮬레이션의 결과는 그림 12와 같다. 콘텐츠 재생권한 라이센스 1개의 증거로도 약 1000개의 에이전트 모듈에서 증거가 전송 될 경우 약 2M정도의 차이를 보인다. 이와 같은 결과는 하나의 에이전트에서 생성한 라이센스 정보의 량에서 차이를 보이므로 당연한 결과라 할 수 있다. 본 실험은 라이센스에 관한 정보만을 추출하여 테스트 하였으나 추후 다른 증거들도 포함될 경우 더 많은 차이를 보일 것이다.



<그림 12> 포렌식스 증거전송 네트워크 트래픽

VI. 결론

네트워크 환경에서는 다양한 방법으로 디지털 콘텐츠가 사용자에 의해 이용된다. 이러한 다양한 환경에서 디지털 콘텐츠의 보호와 함께 불법적인 이용을 탐지하고 대응할 수 있는 기술이 필요로 한다.

본 논문에서는 네트워크 환경에서 안전한 콘텐츠 보호와 유통을 위한 DRM과 디지털 콘텐츠 포렌식스를 지원하는 모델을 제시하였다. DRM 모델은 기존의 MPEG-21 프레임워크를 기반으로 LMS, CMS, CS를 이용하여 안전한 콘텐츠 분배를 가능하게 하였으며, 디지털 콘텐츠 포렌식스 모델은 포렌식스 관리 서버와 에이전트 모듈을 제안하여 컴퓨터 포렌식스 절차를 지원하도록 하였다. 세부적으로 기존의 컴퓨터 포렌식스 모델은 증거 수집을 위하여 특정 폴더 또는 파일, 디스크를 이미지화하여 수집하였다. 그리고 포렌식스 증거물 전송에 있어 네트워크 트래픽을 최소화하기 위한 증거 수집 및 전송 모델을 제안하였다. 본 모델의 성능 평가는 DRM 측면과 포렌식스 측면으로 분류하여 평가하였다. 평가 결과, 본 모델은 MPEG-21의 핵심 사항을 지원하며, 네트워크 트래픽에 낮은 영향을 미쳤다.

본 모델은 침해 및 오용된 디지털콘텐츠에 대한 탐지 에이전트에 의해 로깅 정보가 수집된다. 수집된 증거물이 안전하게 법적 효력을 발휘할 수 있도록 관리하는 네트워크 모델이다. 즉 신뢰된 효율성 있는 증거물이 수집 에이전트에 의해 확보되었다라는 가정하에 네트워크 영역에서 증거물을 안전하게 관리하는 모델이므로 증거 수집 기능 및 포렌식스에 효율적인 증거물 확보 에이전트를 본 모델에 적용한다면 포렌식스에 의한 콘텐츠의 지적재산권 보호에 효율성을 발휘할 것으로 본다.

참고문헌

[1] 전서관, 은선기, 오수현, “상호인증을 제공하는 개선된 RFID 인증 프로토콜,” 전자공학회논문지, 제47권 TC편 제2호, 2010. 2.

[2] 정익래, 홍도원, 정교일, “디지털 포렌식 기술 및 동향,” ETRI 전자통신동향분석 제22권 제1호, 2007. 2.

[3] Lee Garber, “Encase: A Case Study in Computer -Forensics Technology,” IEEE Computer Magazine Jan 2001.

[4] D. Farmer and W. Venema, “The Coroner Toolkit (TCT) v1. 11,” Available at: http://www.Porcupine.org/forensics/tct.thml, September 2002.

[5] TCT: The Coroner's Toolkit, http://www.fish.com/tct

[6] 임의열, 박태규, 최용락, “컴퓨터 포렌식스 절차에 기반한 사용도구 분석,” 한국인터넷학회 학습발표대회논문집, 제5권 제2호, 2004. 11.

[7] Vlastos, E. ; Patel, A., “An open source forensic tool to visualize digital evidence,” Computer standards & interfaces, vol. 30, no. 1/2, 2008.

[8] 장의진, 정병옥, 임형민, 신용태, “안전한 디지털 저작권 관리를 위한 디지털 포렌식 모델 제안,” 정보보호학회논문지, 제18권 제6(A)호, 2008. 12.

[9] Hogab. K., Keunyoung, L., Taehyun, K., “MPEG-21 and Its Interoperability with Rights-Information Standards,” IEEE multimedia, vol. 16 no. 1, 2009.

[10] 정상원, “MPEG--21의 DRM 기술 표준화 현황 분석,” 한국과학기술정보연구원, 정보관리연구, vol. 35, no. 2, 2004.

[11] Lopez, F., Martinez, J. M., Garcia, N., “CAIN-21: An Extensible and Metadata-Driven Multimedia Adaptation Engine in the MPEG-21 Framework,” Lecture notes in computer science, vol. 5887, 2009.

■ 저자소개 ■

장 은 겸
Jang, Eun Gyeom

2009년 3월~현재
대전대학교 컴퓨터공학과 겸임교수
2008년 3월_현재
(주)엠투엠코리아부설기술연구소장
2007년 8월 대전대학교컴퓨터공학과(공학박사)
2002년 8월 대전대학교컴퓨터공학과(공학석사)

관심분야 : 컴퓨터포렌식, DRM, 시스템 접근통제
E-mail : jangegu@nate.com

이 범 석
Lee, Bum Suk

2008년 3월~현재
혜천대 유아교육과 교수
1992년 3월~2008년 2월
혜천대 컴퓨터 멀티미디어과 교수
1998년 2월 성균관대학교 통계학과 전산통계학 (박사)
한국외국어대 정보처리학(석사)

관심분야 : 멀티미디어, 교육공학
E-mail:bslee@hu.ac.kr

논문접수일 : 2010년 3월 8일
수 정 일 : 2010년 4월 21일(1차), 5월 25일(2차)
게재확정일 : 2010년 6월 8일