포렌식 컴퓨팅을 위한 XML 기반 지적 재산권 매핑 시스템

황 철[0] 노 흥 식* 황 대 준
성균관 대학교 전전컴학부 멀티미디어 시스템 연구실
sfo@kookmin.ac.kr djhwang@skku.ac.kr
*협성대학교 컴퓨터공학과
hsnoh@hyupsung.ac.kr

Mapping System of XML-based Intellectual Property Rights for Forensic Computing

Chul Hwang Heung-Sik Noh* Dae-Joon Hwang
Department of Computer Engineering, SungKyunKwan University
*Department of Computer Engineering, HyupSung University

요 약

포렌식 컴퓨팅에 관하여 1984년부터 많은 연구가 진행 되어 왔으며, 이분야 연구는 주로 디스크에 관한 화학적, 물리적 방법을 이용한 증거 추출(Evidence Capture)에 중점을 두어 왔다. 최근 forensic software engineering 분야의 접근은 알고리즘의 error detection에 연구 방향을 두고 있다. 그러나 지적 재산권 법을 온 라인 상에서 컨텐츠를 이용하는 가운데 적용 시키는 연구는 미비하다. 본 연구에서는 지적 재산권을 이용한 XML tree를 만들고, parsing하여 RDB를 구축한 후 질의(query)하여 매핑(mapping)시키는 시스템을 구현 하고자 한다. 입력 자료는 우리가 기존에 개발한 DRM(Digital Rights Management) 시스템에서 사용자를 모니터링하여 검출한 불법 복사/증거 프로 파일로 한다. 이것은 법 전문가에 의뢰하기 전에, 사용되는 컨텐츠가 법에 위배 된다면 지적재산권 법 몇조 몇항에 해당되는지를 사용자, 대리인/변호인, attorney, judge 등에게 컨설팅 해주는 시스템이다.

1. 서 론

컴퓨터 포렌식스는 잠재적인 법적 증거를 결정짓는 컴퓨터 수사와 분석 기술의 응용이다. 여기서 증거는 지적 재산권의 파괴 또는 절도와 사기, 무역 비밀의 절도를 포함하여 컴퓨터 범죄, 오용등 존재 범위가 매우 넓다[2]. 또한 포렌식 컴퓨팅은 법정에서 받아 들일 수 있는 증거를 조사하고, 전자적 근거를 다루고 시험하며 조종하는 방법을 연구하는 과학 분야로서 연구는 주로 disk/tape의 recovery, data conversion, discovery등 물리적, 화학적 방법을 이용한 증거 추출(Evidence Capture)에 중점을 두어 왔다[1,7].

최근에 와서 소프트웨어의 불법복제를 보호하기 위한 기반 기술들의 많은 연구가 진행되고 있다[9]. 본 연구에서는 지적 재산권 법을 분석하여 지적 재산권 위반 사항에 따라서 분류하여 XML 문서를 구축 하였다. 이 XML 문서는 XML 인스턴스의 문법에 해당하는 DTD와 실제 분류된 지적 재산권 법의 내용인 인스턴스로 이루어 진다. 또한 XML 문서는 파싱하여 관계형 데이터 베이스에 저장한다. 이때 XML DTD는 관계형 데이터 베이스의 스키마를 이루고 XML 인스턴스는 테이블의 레코드와 필드를 이룬다.

본 연구에서는 기존에 우리가 개발한 구현한 에이전트 기반의 DRM 시스템[6]에서 사용자를 모니터링하여 불법 사항에 대한 프로파일 정보를 유지하고 있다. 따라서 법에 저촉되는 사항을 모니터링하여 추출한 DRM 시스템의 결과물은 관계형 데이터 베이스에 저장되어 있는 지적 재산권 법 조항에 대한 질의를 위하여 SQL 문으로 입력되고 위반행위에 대한 해당 법 조항을 질의의 결과로서 반환 한다.

RDBMS는 Operation이 실행될 때에 한번 DBMS를 호출(call) 할 때마다 여러 건을 처리하도록 하여 DBMS의 호출 횟수를 줄임으로써, 시스템 오버헤드를 감소시키는 다중처리(Array Processing) 방법이 가능한 오라클을 사용 하도록 한다[5].

2. 관련연구

✧ Data Recovery

컴퓨터가 부팅이 안될 때, 파티션이 없어지고 억세스가 안될 때, 응용 프로그램이 데이터를 load 또는 run 을 못할 때, Corrupted data, disk crash, 바이러스 등으로 인하여 손실이 생겼을 때 회복 시키는 방법이다.

✧ Data Conversion

text/graphics, books, magazines, financial, legal, microfilm 등을 digitized form으로 변환 시키는 방법이다.

✧ 영상처리를 이용한 법 응용
✧ Fragile computer data
✧ Analyze digital evidence
✧ Forensic Software Engineering[3]

- ✧ Forensic Evidence 피공급자
  - ◆ Civil litigations
  - ◆ Insurance Companies
  - ◆ Law Enforcement Officials
  - ◆ Individuals

3. 컴퓨터 포렌식스 절차

주제(subject) 컴퓨터 시스템에 존재 가능한 증거를 단계적으로 검출하고 정의 해 나가는 것이다. 바이러스 침투, 데이터 상실, 손상, 변조가 발생 되는 것으로부터 포렌식 시험을 통한 주제 컴퓨터 시스템을 보호하고 다음 절차를 거친다.

1) 주제 시스템상의 모든 파일의 발견 : 모든 파일은 정상적인 파일, 지워지고 남은 파일, 숨은 파일, 패스워드로 잠긴 파일, 암호화된 파일을 말한다.

2) 발견한 지워진 파일을 가능한 한 모두 복구한다.

3) OS 와 응용 프로그램에 의해 사용된 잠재 파일이나 스왑 파일 또는 숨긴 파일의 컨텐츠를 출현 시킨다.

4) 금기(protected) 또는 암호화된 파일의 컨텐츠를 법적으로 정당하게 접근한다.

5) 디스크의 접근하기 어려운 특별한 영역이라 하더라도 관련있는 가능한 모든 데이터를 분석한다.

6) 관련있는 파일과 발견된 데이터 파일의 리스트와 함께 주제 컴퓨터 시스템의 전반적인 분석 내용을 출력한다[2].

4. 매핑용 증거 추출 시스템(Evidence Detection System for Mapping)

[그림 1]은 디지털 저작권 관리(DRM)시스템 이며 인증 기능은 전자상거래 시스템과 연동되고 저작권 관리 기능은 미션제어, 통계분석 및 지원을 갖고 있으며 감시 및 추적 기능은 ARPA(Adaptive Resource Protection Agent) 에이전트가 수행 한다.

4.1 ARPA 의 특징
- 적응형 에이전트 기반의 저작권 관리 기술
- 온라인 또는 오프라인 환경에서 실시간 감시 및 추적
- 표현 미디어 유형과 무관한 저작권 관리
- 컨텐츠 생성 환경 및 파일 포맷에 독립적
- 환경 적응적인 동적인 저작권 보호
- 인터넷과 인트라넷 기반의 실시간 통계자료 분석 및 관리
- 능동적 자원과 수동적 자원에 일관되게 적용가능
- 컨텐츠와 적용기술의 독립성 유지

DRM 시스템에서 추출된 불법 복사/증거 자료는 RDB 의 입력 자료로 사용된다[6].

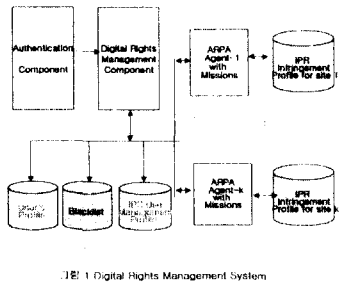
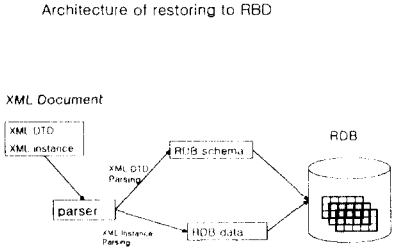


그림 1 Digital Rights Management System

[그림 1] 디지털 저작권 관리(DRM)시스템

5. RDB(Relational DataBase) 저장

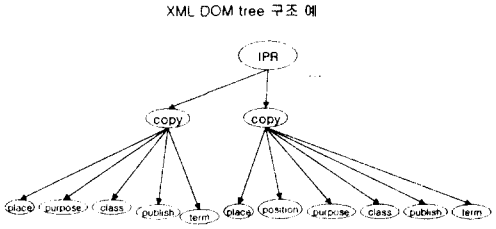
RDB 에 저장되는 과정은 분류되어 있는 XML tree 를 parsing 하여 관계형 데이터베이스에 저장한다. 이 때 XML DTD 와 instance 를 모두 고려하여 저장한다. XML DTD 는 관계형 데이터 베이스의 스키마를 형성하며 XML 인스턴스는 관계형 데이터 베이스 테이블의 레코드와 필드들을 이룬다. RDB 에 저장되는 구조는 [그림 2]와 같다.



[그림 2] RDB에 저장되는 구조

5.1 XML DOM tree 구조

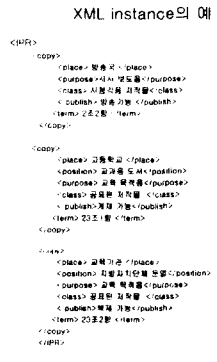
지적 재산권의 대분류는 불법 복제로 했으며 소분류는 복제 장소, 복제 내용, 저작물 종류, 복제 목적, 조항으로 나누었다. 분류 방법은 다양하게 나눌 수 있으며 지적 재산권 전체를 분류하여 대용량의 RDB를 구축 할 수 있다. 본 연구에서는 복제 목적에 의한 분류를 우선시도 하였다. XML DOM tree는 [그림 3] 과 같다.



[그림 3] XML DOM tree 예

5.2 XML 인스턴스

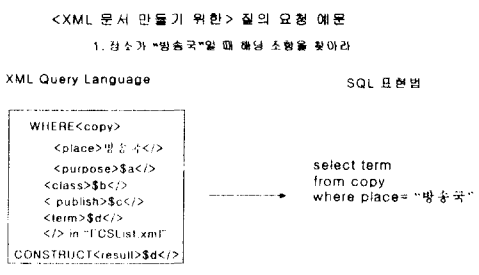
[그림 3]의 DOM tree 예를 이용하여 세부적인 instance를 지적 재산권 법에 적용시켜 만들었다. 내용은 [그림 4]와 같다.



[그림 4] XML 인스턴스 예

5.3 질의 요청

1. 장소가 "방송국"일 때 해당 조항을 찾아라
2. 장소가 "방송국"이면서 목적이 "시사 보도용"일 경우 해당 조항을 찾아라



[그림 5] 질의 및 요청 예문

예문에서 1번에 해당하는 XML Query Language와 SQL 표현 법을 [그림 5]에 나타냈다. 2번은 같은 방법으로 작성 할 수 있으므로 생략 하였다.

6. 결 론

포렌식 컴퓨팅은 지적 재산권에 관련된 법적 소송이 제기 되었을 때 과학적인 방법으로 증거를 제시하여 공신력있는 판결을 유도 할 수 있도록 하는 분야이다.

본 연구에서는 에이전트 기반의 DRM 시스템을 이용하여 사용자들의 불법 사항을 모니터링한 정보와 지적 재산권에 대한 법 조항을 XML로 구축하고 이를 효율적으로 관리하기 위해 관계형 데이터 베이스에 매핑 시킨 과학적인 포렌식 컴퓨팅 시스템을 구축하였다.

향후 이 시스템에 실질적이고 구체적인 증거 질의 시스템을 보강하고 인증 시스템을 추가 함으로서 보다 체계적인 포렌식 컴퓨팅 시스템을 구축 해 갈 것이다.

7. 참고문헌

[1]AuthenTec International, http://www.authentec.co.uk/,

Vogon International, http://www.vogon.co.uk/

[2] Judd Robbin, http://www.computerforensics.net/

[3] Chris Johnson, Forensic Software Engineering : Are Software Failures Symptomatic of Systemic Problems?, Department of Computing Science, University of Glasgow, Glasgow, G12 8QQ, UK.

[4] Forensic Computing: A Practitioner's Guide, Tony Sammes and Brian Jenkinson, Springer-Verlag

[5] 이화식 지음, "대용량 데이터베이스 솔루션", ㈜엔코아정보컨설팅

[6] 황 철 , 황 대준, "디지털 컨텐츠 보호를 위한 에이전트기반 포렌식 컴퓨팅 관리", Proceeding of The 28th KISS Spring Conference, April 27~28, 2001

[7]S.G.R. MacMillan barrister, Toronto, Canada http://www.sgrm.com

[8] 정회경, 홍성찬, 이수연 역, "XML by example", 이한 출판사, 2001년 4월

[9] Workshop on Digital Rights Management for the Web, World Wide Web Consortium, 22-23 January 2001, INRIA - Sophia-Antipolis, France http://www.w3.org/2000/12/drm-ws/