포렌식 컴퓨팅을 위한 XML 기반 지적 재산권 매핑 시스템

원재 * 노홍석 • 황대준
성균관대학교 전산학부 컴퓨터시스템 연구실
stj@korea.ac.kr dhwang@kku.ac.kr
•성균관대학교 컴퓨터ocaust학과
bso@hyupung.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

요약
포렌식 컴퓨팅에 관한 1984년부터 많은 연구가 진행되어 왔으며, 이론과 연구는 주로 디렉터에 관한 파일, 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 법률은 라인상에서 분석을 이용하는 기존에 적용된 방식을 바파하게 한다. 본 연구에서는 지적 재산권을 이용한 XML tree를 만들고, parsing하여 RDB를 구축한 후 질의(query)하여 매핑(mapping)시키는 시스템을 구현하고자 한다. 양식 정보는 우리가 기존에 개발한 DRM(Digital Rights Management) 시스템에서 사용자를 모니터링하여 얻은 정보(복사/복제) 프로 파일화 한다. 이것은 범죄자에 의한 피해과 기계 자동화된 범죄 발생에 해당되는지를 사용자, 해양/법원, 월드, 수사 등에 제공하는 시스템이다.

1. 서론

컴퓨터 포렌식은 잡재적인 법적 증거를 결정짓는 컴퓨 터 사용과 분석 기술의 통합이다. 어떻게 증거는 지적 재산 권의 과정 또는 절도와 사기, 무역 비밀의 절도를 포함하여 컴퓨터 범죄, 오용 등의 범위가 매우 넓다. 또한 포렌 식 컴퓨팅은 법정에서 받아 들인 수 있는 증거로 조사하고, 전자적 기록을 다루고, 시점하여 조증하는 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 외적 소프트웨어의 불법 복제를 보호하기 위한 기 반 기술의 많은 연구가 진행되고 있다. 본 연구에서는 지적 재산권 법률에 기반한 시스템 중 일부에 따라 분석하여 XML 문서를 구축하였다. 이 XML 문서는 XML 인스턴스의 문법에 해당하는 DTD와 실제로 분류된 지적 재산권 법률 인스턴스로 이루어진다. 또한 XML 문서는 과장하여 관계형 데이터베이스에 저장한다.

이제 XML DTD는 관계형 데이터베이스의 스키마를 이루고 XML 인스턴스는 테이블의 레코드와 필드를 이룬다.

본 연구에서는 기존에 우리가 개발한 구현된 예외언어 기반의 DRM 시스템[1]에서 사용자를 모니터링하여 불법 사항에 대한 프로파일 정보를 유지하고 있다. 따라서 범죄에 저촉되는 사용자를 모니터링하여 증거를 주재한 DRM 시스템의 결과물은 관계형 데이터베이스에 저장되어 있는 지적 재산권

법 조항에 대한 결론을 위하여 SQL 문으로 입력되고 정책위에 대한 해당 법 조항을 결론의 결과로서 반영한다.

RDBMS는 Operation에 필요할 때만 DBMS를 호출(call) 할 때마다 여러 건을 처리하도록 하여 DBMS의 호출 횟수를 줄이며, 시스템 오버헤드를 감소시키는 다중처리(Array Processing) 방법이 가능 한 실용성을 사용하도록 한다[5].

2. 관련연구

♦ Data Recovery

컴퓨터가 부팅가 안될 때, 파라미터가 없어지고 범죄자가 인터넷에, 응용 프로그램의 데이터를 load 또는 run을 못할 때, Corrupted data, disk crash, 바이러스 등으로 인해 손실이 생겼을 때 회복을 목적으로 하는 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[13]

655
3. 컴퓨터 포렌식 절차

주체(subject) 컴퓨터 시스템에 존재 가능한 증거를 단계적으로 검출하고 정의해 나가는 것이다. 마이크로 휴대, 데이터 성장, 손상, 변조가 발생 되는 것으로부터 포렌식 시험을 통해 주체 컴퓨터 시스템을 보호하고 다음 절차를 거친다.
1) 주체 시스템상의 모든 파일의 발견: 모든 파일은 정상적인 파일, 지위를 지나 넘은 파일, 숨은 파일, 폴더, 폴더 잡간 파일, 암호화된 파일, 같은 파일을 만든다.
2) 발견된 지위 파일을 가능한 한 모두 복구한다.
3) OS 와 응용 프로그램에 의한 사용된 잠재 파일이나 스할 파일 또는 숨긴 파일의 컨텐츠를 충전 시킨다.
4) 급기(protected) 또는 암호화된 파일의 컨텐츠를 법적으로 정당하게 접근한다.
5) 다스크의 접근하기 어려운 특별한 영역이라 하더라도 관리는 가능한 모든 데이터를 분석한다.
6) 관련있는 파일과 발견된 데이터 파일의 리스트와 함께 주체 컴퓨터 시스템의 전반적인 분석 내용을 줄린다[2].

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

[그림 1]은 디지털 저작권 관리( DRM) 시스템이며 인증 기능은 진지상거래 시스템과 연동되고 저작권 관리 기능은 미션체어, 통계분석 및 보안을 갖고 있으며 보안 및 저작권 기능은 ARPA(Adaptive Resource Protection Agent) 예인천이 수행 한다.

4.1 ARPA의 특징
- 적용형 저작권 기반의 저작권 관리 기술
- 스마트 또는 오프라인 환경에서 신고사항 검사 및 주
- 표준에 따라 유형의 정점을 저작권 관리
- 컨텐츠 생성 및 파일 모드에 독립적
- 적용 가능한 동적인 저작권 보호
- 인터넷과 인터넷 기반의 신고 통계자료 분석 및 관리
- 동등적인 자원과 복제된 자원에 이관되지 적용 가능
- 컨텐츠와 적용기술의 독립성 유지

DRM 시스템에서 추출된 법적 복사/증거 자료는 RDB의 입력 자료로 사용된다[6].

5. RDB(Relational DataBase) 저장


Architecture of restoring to RDB

[그림 2]에 저장되는 구조

5.1 XML DOM tree 구조

저작 재산권의 대체를 루트 벡으로 했으며 소분류는
복제 정책, 복제 내용, 저작물 종류, 복제 목적, 조합으
로 나누었다. 분류 방법은 다양하게 나눌 수 있으며 저작
재산권 전체를 분위하기 대용량의 RDB를 구축할 수 있다. 본 연구에서는 복제 목적에 의한 분류를 우선
시도 하였다. XML DOM tree는 [그림 3]과 같다.
5.2 XML 인스턴스


[그림 4] XML 인스턴스 예

5.3 절의 요청

1. 장소가 "방송국"일 때 해당 조항을 찾아야 한다.
2. 장소가 "방송국"이면서 모든이 "서사 보도용"일 경우 해당 조항을 찾아야 한다.

```
<XML 문서 만들기 및 사용 조항 요청 예문>
1. 장소가 "방송국"일 때 해당 조항을 찾아야 한다.
```

6. 결론

아래 내용에서 1번에 해당하는 XML Query Language와 SQL 표현 방식 [그림 5]에 나타났다. 2번은 같은 방법으로 작성할 수 있으므로 생략하였다.

```
[그림 5] 질의 및 요청 예문
```