디지털 컨텐츠 보호를 위한 에이전트기반 포렌식 컴퓨팅 관리

황 철° 황대준

성균관대학교 컴퓨터공학 부 멀티미디어시스템연구실

sfc@kookmin.ac.kr djhwang@yurim.skku.ac.kr

Agent-based Forensic Computing Management for Protection of Digital Contents

Chul Hwang° Dae-Joon Hwang

Dept. of Computer Engineering, Multimedia System Lab.

SungKyunKwan University

요 약

지적 재산권 보호 중에서 디지털 저작물 보호는 근래에 활발히 연구되고 있으며 법 과학 분야는 지문감식, 치아감정, DNA 등 많은 분야가 있다. 법과학 분야중 법적용 컴퓨팅(Forensic Computing)에 관한 응용은 새로운 연구 과제이다. 그중에도 디지털 저작물에 대하여 증거를 보전 하고자 많은 연구가 진행 되고 있지만 디지털 저작물에 관하여 네트워크를 통한 능동적 저작물 보호는 미약하다. 현재의 데이터 추출(Extraction), 발굴(Exploitation), 복구, 암호 해독, 패스워스 풀기(Defeat), 미러 이미징 등의 방법 가지고 해결 못하는 경우와 인터넷 상에서 온라인으로 이루어지는 불법 복제에서 결정적 기여(smoking gun)를 찾아 내려고 하는 것이 본 논문에서 해결 하고자 하는 부분이다. 오프라인일 경우도 가능하며 분석된 결과는 변호사/대리인, 법인, 보험회사, 법집행관 등에게 온라인으로 제공한다. 진행 과정은 서버에서 파견 시킨, 미션을 부여 받은 에이전트가 저작물 불법 복제 상황을 트래킹 한 후, 네트워크를 통하여 정해진 시간별로 서버에 전달하면, 법 조항과 매핑시켜서 분석한 다음 서버의 지식베이스에 저장되어 사용자의 요구에 응하는 능동형 디지털 저작물 보호 관리 시스템이다.

1. 서론

법과학은 감정/감식에 관한 과학을 총칭하며 구체적으로는 법의학, 법의병리학, 법의 혈청학, 법이화학, 법생물학, 문서감정학, 거짓말탐지학, 유전자감식학 등의 분야로 나눌수 있다. 과학수사에서 감정 감식은 과학지식과 기술을 이용하는것이며 감정은 감정인의 주관적인 경험과 지식을 위주로 한 판단(문서감정, 음성감정 등), 감식은 객관적인 과학적 결론을 위주로한 판단(유전자감식, 마약감식 등)으로 구분되나 모두 감정 또는 분석이라고 한다. 과학수사는 범인의 식별, 증거의 수집분석등 수사의 가장 중요한 분야에 결정적 기여를 할 수 있다.

과학수사는 과학의 폭넓은 응용으로 주변과학의 발전에 따라 새로운 과학수사의 방법이 개발되어 1960년대에 원자력에 의한 중성자 방사화 분석이 개발되었고, DNA의 구조에 관한 분자 생물학의 연구가 범인 식별법으로 각광을 받고있다[9].

본 연구에서는 최근에 과학수사에 많은 영향을 끼치고 있는 정보통신 공학분야 중에서 디지털 컨텐츠를 보호하고 법적 증거로서 수사에 적용되는 포렌식 컴퓨팅을 제안한다. 또한 지적재산권의 디지털 저작물을 보호하기 위해 능동적이며 실시간으로 모니터링하여 보호하며 불법복제에 대하여 제재를 가하기 위한 서버 클라이언트 DRM(Digital Rights Management)시스템을 개발한다. DRM 시스템은 오디오의 MP3, AAC, WMA 파일, 비디오의 MPEG, WMA, AVI, MOV 파일, 문서 파일, 이미지 파일, 원격 강의용 파일, 웹문서, 만화 등 많은 곳에 응용된다. 본 논문에서의 주안점은 기존의 인증키를 사용하는 대신 트래킹 기법을 적용 시키고 DRM 시스템에 포렌식 컴퓨팅을 적용시키고자 하는것이다. 즉, 인터넷을 통하여 모니터링하고 증거를 수집하여 데이터 베이스를 만든다음 법적 내용과 1:1 매핑시켜 사용자의 요구에 응하는 시스템이다[2].

2. 관련연구

지적 재산권 보호방안으로는 기존의 법체계에서의 저작권 보호를 들 수 있으나 이 경우 법적인 문제는 사후의 구제수단과 실제적인 방지책으로는 한계가 있다. 따라서 실제적으로 보호 할 수 있는 방안으로 암호화 기법, 정보에 대한 접근제어, 디지털 워터마킹 기법 등을 활용 한 수 있을 것이다. 그 외에 해킹 시스템의 불법적인 사용을 탐지 해내는 시스템인 IDS(Intrusion Detection System)와 지적 재산권의 디지털 사용에 대한 법적인 증거 개념인 포렌식 컴퓨팅을 들 수 있다.

2.1 암호화 방식

암호화는 전자서명 및 정보보안의 기본적인 기술이라고 할 수 있으며 데이터를 암호화하는 방식은 대칭과 비대칭 암호화 방식의 기본적인 형태가 있다. 대칭 암호화 방식은 암호화하는 키와 복호화하는 키가 동일한 경우이며, 비대칭 암호화 방식은 키를 공개하기 때문에 공개키 암호화 방식이라고 말하며 암호화하는 키가 서로 다른 경우이다.

암호화 프로그램의 특성으로는 범용성을 지녀야하고, 특정키만 입력하면 기계적으로 암호화와 복호화가 가능 해야하고, 보안성이 유지되어야한다[10].

2.2 워터마킹(watermarking) 방식

워터마크는 저작권 보호를 위해 쓰이는 영상 데이터에 표시된 보이지않는 마크를 의미한다. 워터마크의 중요한점은 어떤 경우라도 워터마크를 추출할 수 있어야한다. 공간영역에서 워터마크를 삽입하는 방법은 임의의 픽셀 값의 LSB를 변형시키는 것이며 잡음과 원래 신호와의 처리가 매우 민감하다. 주파수 영역에서의 디지탈 워터마크 방법은 영상 데이터를 FFT, DCT, Wavelet 등과 같은 변환으로 주파수 공간에서 시각적으로 덜 민감한 성분에 워터마크를 삽입하는 방법이다[4].

2.3 접근제어 방식

허가되지 않은 자원(불법적인 자원의 사용, 노출, 수정, 파괴, 불법 명령)에 대하여 접근을 통제하는 방식이며 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용에 대하여 권한 부여를 위한 수단이다.

2.4 침입 탐지 시스템(Intrusion Detection System)

ID 시스템은 침입의 패턴 데이터 베이스와 전문가 시스템을 사용하여 네트워크나 시스템의 사용 상황을 실시간으로 모니터링하고 침입을 탐지하는 보안 시스템이다.

3. DRM(Digital Rights Management) 시스템 구조

본 연구에서 개발한 DRM시스템에서 법적용에 포함될 내용은 오디오/비디오 도큐먼트, 절차형 도큐먼트, 명백한 로깅, 모든 미디어 타입으로부터 획득한 증거, 상세한 증거를 가진 보고서 등이고 사용된 DRM 시스템은 관리 서버와 클라이언트 에이전트로 구성된 능동형 컨텐츠 보호 프레임 워크이다. 법적용 방법은 소프트웨어의 업그레이드 판을 다운받도록 허용하게 할 때 고객의 레벨에 따라 허용 횟수를 정하고, 허용범위를 넘었을 때 일단 경고를 주고, 반복될 때는 설정 해놓은 증거 히스토리를 이용하여 로그 파일로 만들어 데이터 베이스에 저장시킨다. 오토너머스 필터링을 하기 위하여 각각의 이벤트에 따라서 사안별로 고객의 레벨별로 파일 이름, IP 번호, 복사회수 등의 모든 조건을 종합하여 개별 임계점을 정한 후 법적용을 시키도록 하는 것이다.직용시킬 법의 종류,고객 레벨에 대한 임계점을 수정함으로써 저작권자가 서버를 이용할 수 있다.

3.1 관리 서버(Management Server)

고객이 공급받은 컨텐츠를 합법적으로 사용하는지를 모니터링하기위해서 미션을 부여받은 에이전트가 파견되어 있다. 인터넷으로 온라인 상태가 되면 에

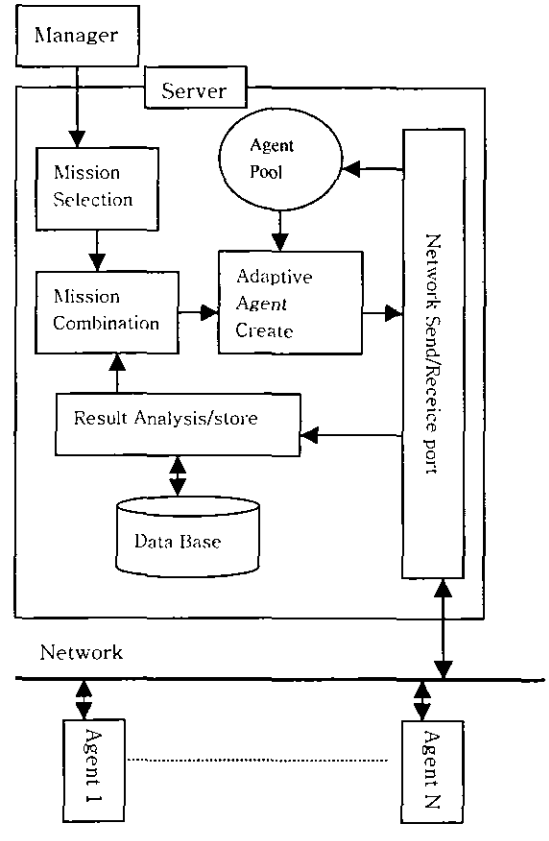

그림 1 관리 서버 구조

이전트가 동작하여 고객의 불법적인 사용에 관련된 내용을 서버에 보고하고 지시에 따라 액션을 취한다.

그림1에서 보는 바와 같이 클라이언트(컨텐츠 사용자)에 파견(delegate)된 에이전트들에게 여러가지 미션(mission)을 실시간으로 주고 결과를 취합하여 보고 받는다[2]. 보고된 결과를 바탕으로 새로운 미션을 부여 할 수 있고 분산 시스템으로 이루어져 있으며 기초 통계 자료가 만들어 진다[10]. 관리자의 편의를 위한 네트워크 툴이나 GUI 환경을 제공한다.

3.2 에이전트 클라이언트(Agent Client)

그림 2에서 보는 바와 같이 에이전트는 모니터링 해야할 컴퓨터에 소프트웨어/컨텐츠와 함께 동승시켜 파견한다[8].

파견된 에이전트는 서버에서 부여한 미션을 수행한다. 미션은 클라이언트 쪽의 자원들을 보호하고, 감시(Surveillance) 해야할 임무와 명령을 의미한다.

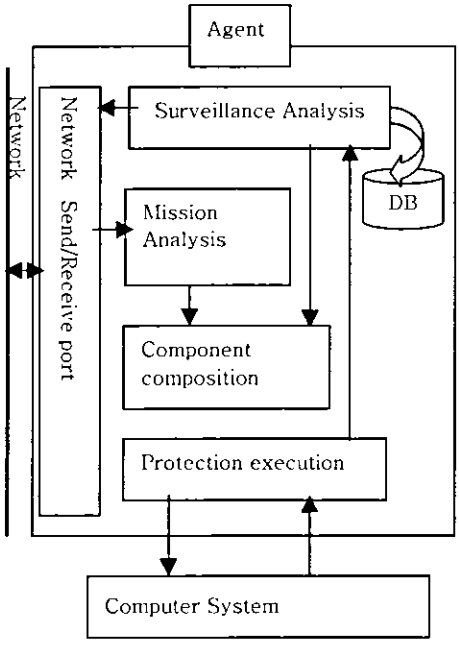

그림 2 에이전트 클라이언트 구조

클라이언트에서 수행된 결과는 온 라인 상태일때는 서버에게 보고하고 오프 라인 상태에서는 클라이언트 컴퓨터의 임의의 장소에 결과를 저장한다.

4. 결론

기존의 정보보호 모델인 암호화 기법, 워터마킹 그리고 접근제어 기법들은 암호 이론을 기반으로 하였다. 암호문은 암호화 시키는데 걸리는 시간이 길며 불법 행위의 입증에 필요한 법적 자료 확보가 불가능하다. 본논문에서는 저작자의 디지탈 컨텐츠를 누가, 언제, 어디서, 어떻게 사용 하는지를 계속 추적해 가면서 법적 증거를 확보해 놓는 시스템이다. 이와같은 능동적 컨텐츠 보호, 감시, 추적 방법이 모든 경우의 불법적 복제 방지를 해결할수는 없을지라도 네트워크 상으로 실시간 가능한 장점이 있다. 네트워크가 연결되지 않은 컴퓨터 시스템의 경우 오프 라인에서도 가능하다. 증거를 이용한 실제적인 법 적용에 있어서 법 전문가의 다양한 법논리가 보강 될수록 더욱 완벽한 지능형 디지털 저작물 법적 보호 시스템이 될 것이다.

5. 참고 문헌

[1] Chul Hwang, Yong Hyo Lee, Dae Joon Hwang, "Protection of Digital Contents on Distribution Multimedia Environment", IASTED IMSA 2000, November 19-23, 2000, Lasvegas, Nevada, USA

[2] Lori L. Scarlatos, "Designing Interactive Multimedia", Proceedings of the Fifth International Multimedia Conference, Seattle, Washington, USA, Nov. 1997.

[3] Peter G. Viscarola & W.Anthony Mason, Windows NT Device Driver Development, Macmillan Technical Pub, 1999.

[4] Kallmaker & Karin, Watermarking, Naiad Press, 1999.

[5] Mihai Barbuceanu and Mark S. Fox, "Integrating communicative action, conversations and decision theory to coordinate agents", Proceedings of the first international conference on Autonomous agents, February 5-8, 1997, Marina del Rey, CA USA, pp 49-58.

[6] Jeffrey M. Bradshaw, "Software Agents", AAAI Press/The MIT Press, 1997

[7] Sussman, V. "Policy Cyberspace." U.S. News & World Report, January 23, 1995, pp 55-60.

[8] 동수환, 황대준, "동적 자원 보호 에이전트 특허 문서"

[9] 정상조, "멀티미디어 소프트웨어 제작자의 권리", 서울대학교

[10] C. Ko, M. Ruschitzka, and K. Levitt, "Execution Monitoring of Security-critical Programs in Distributed Systems: A Specification-based Approach" Proceedings of the 1997 IEEE Symposium on Security and Privacy, pp. 134-144