2006년도 대한전자공학회 하계종합학술대회 제29권 제1호

핑거프린팅 기법을 이용한 불법 콘텐츠 추적 시스템

김원겸*, 서용석, 이선화
한국전자통신연구원 DRM 연구팀

Illegal Contents Tracing System using Fingerprinting Scheme

Won-gyum-Kim*, Yong-seok Seo, Seon-hwa Lee
Electronics and Telecommunications Research Institute
E-mail : wgkim@etri.re.kr

I. 서론

최근 디지털 기술과 인터넷 환경의 급속한 발전으로 인해 디지털 콘텐츠의 제작과 판매가 활발해지고 있다. 그러나 손실 없이 대량 복제가 가능한 디지털 콘텐츠의 특성과 사용자들의 유료 콘텐츠 사용에 대한 인식 부족으로 디지털 콘텐츠의 지적재산권 침해가 빈번히 발생하여, 콘텐츠 산업 발전을 저해하는 심각한 문제로 대두되고 있다.

암호화에 근간을 두고 있는 일반적인 DRM 은 콘텐츠에 대하여 지불을 하지 않은 일반 사용자들의 접근자체를 봉쇄하지만, 암호화가 풀린 이후의 상황에서는 콘텐츠의 보호가 사실상 어렵게 된다. 실제로 음악파일이나 동영상 같은 멀티미디어 콘텐츠의 경우 복호화 된 상태나 혹은 콘텐츠의 재생시 다시 캡쳐(capture) 되어 암호화되지 않고 배포되는 경우가 대부분이다.

핑거프린팅 기법은 콘텐츠에 동일한 저작권 정보를 삽입하는 워터마킹 기법과는 달리 사용자마다 각기 다른 정보를 콘텐츠에 삽입함으로써 불법 복제 및 유통행위가 발견되었을 때 불법 배포자를 추적하고자 하는 기술로, 저작권 정보만을 이용하는 워터마킹보다 보다 적극적인 의미의 보호 기법이라 할 수 있으며 부정자 추적(traitor tracing) 기술로도 논의될 수 있다.

본 논문에서는 인터넷 상에서 다량으로 배포된 불법 콘텐츠를 멀티미디어 검색 에이전트를 이용하여 추적하고 이 콘텐츠로부터 핑거프린팅 정보를 추출하여 불법 배포자를 추적하기 위한 시스템 설계를 제안한다.

II. 불법 복제 추적 시스템의 설계

불법 복제 콘텐츠를 추적하기 위해서는 핑거프린팅 기법과 검색 에이전트와의 연동이 필수적이다. 본 장에서는 핑거프린팅 기법과 검색 에이전트를 어떻게 연동하여 불법 콘텐츠를 추적할 것인가를 설명한다.

II-1 핑거프린팅 정보 삽입

콘텐츠 구매 요청 발생시 핑거프린팅 정보를 삽입하여 배포하는 과정은 그림 1 과 같이 이루어진다. 먼저 콘텐츠 제작자(provider)가 판매하고자 하는 콘텐츠를 핑거프린트 서버에 등록한다. 구매자가 콘텐츠 판매자(distributor)를 통하여 구매 요청을 하면 콘텐츠 판매자는 핑거프린트 서버에 구매자 정보를 보내어 핑거프린팅된 콘텐츠, 즉 구매자의 정보가 삽입된 콘텐츠를 받아온 후 다시 구매자에게 보내는 과정을 거친다.

핑거프린팅의 핵심 요구 사항 중의 하나인 비대칭성을 확보하기 위해서는 콘텐츠 판매자가 아닌 제 3 의 공인된 인증 기관에서 핑거프린팅 정보를 삽입하여야 하며, 이로써 정당한 구매자들이 판매자의 비윤리적인 행위로부터 보호받을 수 있다.

512 x 512 크기 이상의 이미지에 대해서 평균화, 모자이크 등의 공모 공격에 강인한 핑거프린팅 삽입 알고리즘을 이미 개발하였으며, 특히 잘라내기와 비슷한 효과를 가지는 모자이크 공격에 대해서는 우수한 결과를 나타내고 있다. 이 핑거프린팅 알고리즘을 활용하여 핑거프린팅 정보를 삽입하고자 한다.

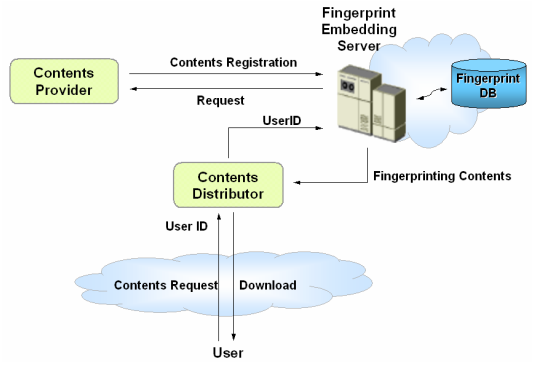

그림 1. 핑거프린팅 정보 삽입

2.2 멀티미디어 검색 에이전트를 이용한 불법 콘텐츠 수집

불법적으로 복제되어 배포된 디지털 콘텐츠의 저작권자 또는 소유권자의 요청으로 불법 복제 콘텐츠를 검색하기 위해 멀티미디어 검색 에이전트를 이용한다. 에이전트는 인터넷상에서 외부로부터 접근 가능한 컴퓨터 시스템들을 돌아다니면서 원본 콘텐츠와 유사한 특성 및 크기를 가진 콘텐츠들을 핑거프린트 추출 서버로 전송한다.

검색 에이전트는 크게 링크 정보 검색부와 콘텐츠 수집부로 나누어지며, 에이전트는 링크 정보 DB 내의 링크들을 주기적으로 방문하면서 새로운 링크 정보 추가, 링크 validation 확인 등을 통해 지속적인 업데이트를 수행한다.

2.3 실시간 핑거프린팅 정보 추출

불법 복제된 콘텐츠를 검색하고 선정된 콘텐츠를 전송하는 과정에서 필수적으로 요구되는 과도한 네트워크 트래픽 부하를 줄이기 위해 검색 에이전트로부터 전송되어 오는 콘텐츠의 일부 내용에서 핑거프린팅 정보를 실시간으로 추출하여 정보가 추출되지 않거나 원본 콘텐츠와 관련없는 정보가 추출될 경우 콘텐츠의 전송을 중지키시고 다른 콘텐츠의 전송 내용을 검사한다.

2.4 불법복제 행위자 추적 및 리포팅

핑거프린트 검색 서버로 전송되어진 콘텐츠들에서 워터마크 형식으로 들어있는 핑거프린팅 정보를 추출하여 불법 복제 행위에 대한 책임자를 판별하게 된다.

일반적인 워터마크에 대한 공격인 압축, 잘라내기, 회전, 크기변경, 변환 등의 공격하에서도 핑거프린트 정보를 추출할 수 있어야 하며, 다수의 공모자에 의한 공모 공격이 가해졌을 경우에는 복수의 사용자 정보를 추출할 수 있어야 한다. 최종적으로는 불법 복제 및 배포 행위의 책임자들을 원본 콘텐츠의 저작권자 또는 소유권자에게 알려주는 리포팅 기능을 갖추어야 한다.

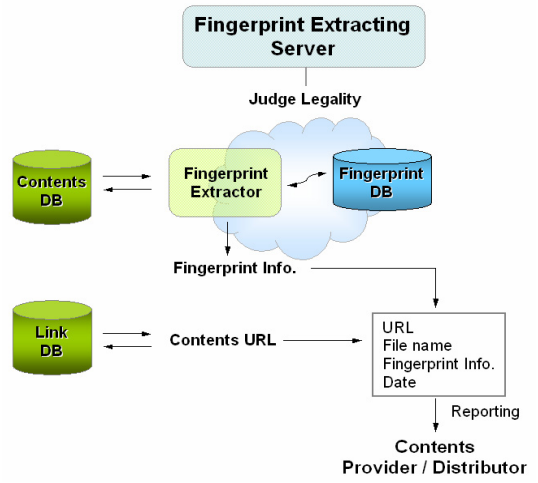

그림 2. 핑거프린팅 추출 및 불법 배포자 추적

III. 결 론

본 논문에서는 핑거프린팅 기법을 이용하여 비대칭성을 만족하는 핑거프린팅 삽입 시스템을 제시하고, 일반적인 텍스트 기반의 검색 에이전트와는 달리 웹상에서 멀티미디어를 검색하기 위한 에이전트가 고려해야 할 사항들을 살펴보았다. 또한 검색된 불법 콘텐츠로부터 핑거프린팅 정보를 추출, 적법성 여부를 판별하고 불법 복제 행위자를 추적하기 위한 시스템의 설계를 제안하였다.

참고문헌

[1] J. Dittmann, P. Schmitt, E. Saar, J. Schwenk, and J. Ueberberg, “Combining digital Watermarks and collusion secure Fingerprints for digital Images.”SPIE Journal of Electronic Imaging, vol.9, pp.456-567, 2000.