이미지 컨텐츠 접근 제어를 위한 DRM 적용방법 설계*

*강정호°, *윤미연, *피영수, *신용태, **장의진
*숭실대학교 컴퓨터학과, **(주)디지캡스
{*kjho80, *myyoon, *coolps, *shin, **fiatlux}@cherry.ssu.ac.kr

A Design of DRM Solution for Image Access Control

*Jungho Kang°, *Miyoun Yoon, *Youngsoo Pee, *Yongtae Shin, **Uijin Jang,
*Dept. of Computing, Soongsil University, **Digicaps

요 약

디지털 컨텐츠의 생산과 수요가 폭발적으로 증가함에 따라 컨텐츠에 대한 지적 재산권 및 수익 창출에 대한 중요성이 대두되었다. 이를 위해 디지털 컨텐츠 자체에 저작권을 보호할 수 있는 기능을 부여하는 기술인 DRM이 개발되었다. 본 논문에서는 DRM(Digital Rights Management)의 영역에 속하는 디지털 컨텐츠 접근을 제어하기 위한 기술 중에서 이미지 컨텐츠에 대한 불법적인 캡쳐 방지를 위한 모델을 제안한다.

1. 소 개

인터넷이 보편화 됨에 따라 기존에 존재하던 아날로그 컨텐츠가 빠른 속도로 디지털 형태의 컨텐츠로 대체되고 있다. 이로 인해 디지털 컨텐츠를 기반으로 하는 사업 영역이 매우 큰 규모로 성장하였고 수익 창출 및 저작권에 대한 중요성이 대두되었다. 하지만 디지털 컨텐츠는 디지털 기술의 특성상 아날로그 컨텐츠에 비해 복제가 매우 쉽기 때문에 새로운 방식의 컨텐츠 보호 기술이 필요하게 되었다. 이를 위해 각종 디지털 콘텐츠에 저작권을 표기하는 워터 마킹이나 불법복제가 이루어지지 않도록 방지하는 DRM(Digital Right Management) 기술이 발전되었다. 국내의 경우 DRM 포럼[6]이 결성되어 클리어링 하우스 기능 연구, DRM API 기능 제시등과 같이 활발한 연구 개발이 수행되고 있다.

본 논문에서는 DRM상에서 컨텐츠의 접근을 제어하는 기술 중에서 이미지에 대한 불법적인 캡쳐 방지 모델에 대해서 다루고자 한다. 컨텐츠에 대한 불법적인 접근의 대부분은 사용자의 PC상에서 이루어지는 까닭에 제안하는 모델 역시 사용자의 PC상에서 효과적으로 이미지 컨텐츠를 보호하는 방법에 중점을 두고 있다. 또한 운영체제와 밀접한 연관을 가지며 작동하는 본 모델은 기존의 컨텐츠 중심적인 보호 기법과 병행하여 사용될 경우 그 효과가 더욱 크게 된다.

본 논문의 2장은 모델을 제안하게 된 배경에 대해서 설명하며, 3장에서는 모델의 설명에 앞서 선행되어 연구된 기술들에 대해 서술하였다. 4장에서는 제안하는 모델을 구성하는 컴포넌트들과 흐름에 대해 설명하였으며 5장에서는 논문의 결과로 끝을 맺는다.

* 본 논문은 현재 산학연 컨소시엄에서 지원하는 과제 번호 "S0305110-A0130115-13013011"의 연구 결과입니다.

2. 연구 배경

DRM에서 컨텐츠 복제를 막기 위해 사용하는 고전적인 형태의 보호 기법은 컨텐츠 자체에 대한 암호화가 있다. 컨텐츠를 암호화함으로써 복제가 이루어진 경우에도 인증 및 복호화에 대한 정보를 가진 합법적인 사용자만이 컨텐츠를 사용할 수 있는 것이다. 하지만 공격 방법이 점차로 고도화 되고 있는 현재 시점에서 어떠한 암호화 기법도 완벽한 안정성을 보장할 수는 없다. 설령 완벽한 암호화 기법이 존재하는 경우라 할지라도 컨텐츠가 정상적인 인증과 암호화 절차를 통과하여 뷰어 상에 보여지게 된 후에는 캡쳐 프로그램과 같은 허용되지 않은 접근으로부터 컨텐츠를 보호 할 수 없다.

위와 같은 문제점들을 해결하기 위해서 사용자들의 PC상에서 시도되는 불법적인 컨텐츠 접근 및 복제로부터 컨텐츠를 보호할 수 있는 방법이 모색되어야 한다. 이러한 문제의 해결책으로 본 논문에서는 사용자의 PC상에 존재하는 컨텐츠 중에서 이미지에 대한 불법적인 복제를 막기 위한 방법을 제시하고자 한다. 제안하는 모델의 기본적인 아이디어는 이미지 캡쳐가 운영체제와 밀접한 연관을 통해서 이루어진다는 것이다. 운영체제가 제공하는 인터페이스를 통해서 캡쳐 기능이 수행되는 만큼 이러한 측면을 이용하여 효과적으로 이미지 컨텐츠의 복제를 제어할 수 있다.

3. 관련 연구

3.1. DRM(Digital Rights Management)

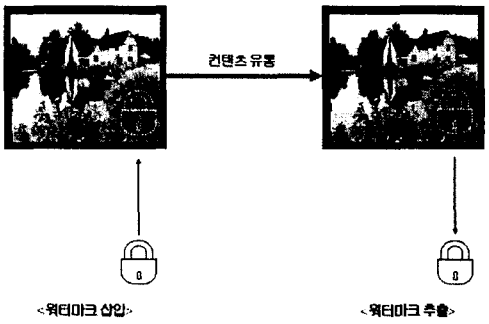
DRM(Digital Rights Management)이란 디지털 형태의 컨텐츠를 안전하고 신뢰성 있는 방법을 통해 관리 유통하기 위한 저작권 보호 체계이다[6]. 순수 디지털 컨텐츠는 디지털의 특성상 컨텐츠의 사용자에 대해 사용상의 제한을 가할 수 없으며, 일단 한번 유통된 컨텐츠에 대해서 더 이상 과금을 할 수 없다. 이러한 한계점을 보완

하기 위해서 등장한 것이 DRM이며 다음과 같이 나누어 질 수 있다.

첫 번째는 사용 측면을 고려한 DRM 시스템으로, 가장 전통적인 방식이며 사용자가 컨텐츠를 사용하는데 있어서 제한을 가하는 것이다. 제한을 위해서 복제 방지 기법이 사용되며 대표적으로 컨텐츠 자체를 암호화 하는 방식을 사용한다. 이는 불법적인 컨텐츠 공유를 어렵게 하거나 불가능하게 한다.

두 번째는 과금 측면을 고려한 DRM 시스템으로 컨텐츠의 이동을 감시하고 추적하는 기능이 필요하다. 이를 위해서 컨텐츠 자체에 워터마크를 삽입하거나 핑거프린트를 추가하는 기법을 사용한다. 이를 통해 해당 컨텐츠에 대한 저작권을 증명하며 불법적인 소유에 대해서 판명할 수 있다[2].

3.2. 워터 마킹



[그림 1] 워터 마킹의 예

이미지 접근 제어를 위해서 사용하는 일반적인 방법으로는 워터 마킹 기법을 사용한다. [그림 1]에서 보는 바와 같이 워터 마킹이란 디지털 컨텐츠의 데이터에 특별한 마크를 삽입하는 방식으로 컨텐츠에 대한 저작권이나 소유권을 의미하는 것이다. 이렇게 삽입된 마크는 일반적인 경우에는 식별할 수 없으나 불법적인 방식으로 컨텐츠를 사용한 경우에 마크를 추출하여 소유를 명확히 할 수 있는 방식이다.

디지털 데이터에 대한 워터 마킹 기술로는 다음과 같은 방식들이 존재한다.

- 이미지 데이터에 대한 체크섬 값을 특정 픽셀의 비트에 삽입하는 방식 [3]
- 별도의 비쥬얼 채널을 사용하여 이미지와는 독립적인 워터마크를 사용하는 방식 [4]
- JPEG 계수를 변조시켜 워터 마크를 생성하는 방식 [5]

위에서 나열한 워터마킹 기법들은 눈으로 보이지 않도록 하거나 일반적인 노이즈처럼 컨텐츠에 워터 마크 정보를 혼합하는 방식들이다[1].

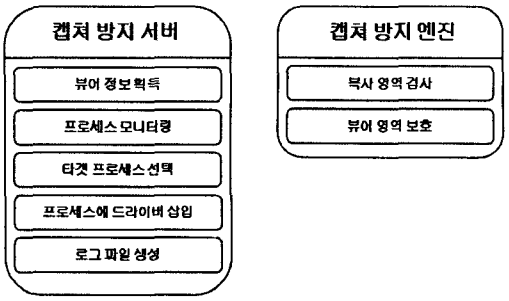
위와 같이 컨텐츠를 암호화 하는 방식은 올바른 복호화와 인증 절차가 끝난 후의 접근 제어에 대해 매우 취약하다. 또한 워터 마킹 역시 소극적인 방식으로 저작권을 보호하는 기술이다. 이러한 까닭으로 컨텐츠를 보호하기 위해서 DRM시스템이나 컨텐츠 자체만을 고려하는 관점이 아닌 사용자의 PC 차원의 관점에서도 문제를 생각해 보아야 한다. 본 논문에서는 보다 적극적으로 이미지 컨텐츠를 보호하기 위해서 운영체제와 연계하여 사용자의 PC상에서 이루어지는 캡쳐와 같은 불법적인 접근을 근본적으로 막을 수 있는 모델을 제안한다.

4. 제안 시스템

본 논문에서는 이미지 컨텐츠의 사용 제한을 위한 복제 방지 기법이 사용된 시스템을 제안한다. 기본적으로 사용자의 PC 상에서 실행되는 프로그램은 운영체제가 제공하는 기본 라이브러리를 사용한다는 것을 전제로 한다.

4.1. 시스템 구성도

본 논문에서 제안하는 시스템은 캡쳐 방지 서버와 캡쳐 방지 엔진으로 나누어진다. 아래의 [그림 2]는 시스템을 구성하는 요소들과 수행하는 기능을 나타낸 것이다.

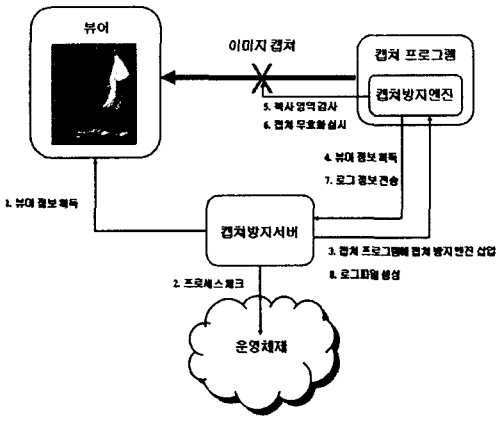


[그림 2] 이미지 캡쳐 방지 시스템 구성요소 및 기능

캡쳐 방지 서버는 일종의 데몬 형태로 항상 사용자의 PC상에서 실행상태에 있어야 한다. 수행하는 기능은 크게 다섯 가지로 나누어 볼 수 있다. 첫째, 뷰어 정보 획득으로 시스템 상에서 DRM이 적용된 컨텐츠를 재생할 수 있는 뷰어의 정보를 수집한다. 수집된 뷰어들은 본 시스템에서 이미지 복사 방지를 적용할 대상이 된다. 둘째, 프로세스 모니터링으로 타겟 프로세스 선택을 위해 시스템 상에서 새롭게 실행되는 프로세스나 실행 상태에 있는 프로세스를 모니터링 한다. 셋째, 타겟 프로세스 선택으로 프로세스가 캡쳐 프로그램으로 의심되는 라이브러리의 함수를 포함하고 있는지를 체크하여, 해당될 경우 타겟 프로세스로 선별한다. 넷째, 프로세스에 캡쳐 방지 엔진 삽입으로 타겟 프로세스로 선정된 프로세스에 캡쳐 방지 엔진을 삽입한다. 다섯째, 로그 파일 생성으로 프로세스들에 삽입된 캡쳐 방지 엔진으로부터 받은 로그 정보를 이용하여 로그파일을 생성한다. 로그는 불법적인 이미지 복사 시도를 한 프로세스에 대한 정보를 포함한다.

캡쳐 방지 엔진은 캡쳐 방지 서버에 의해서 대상 프로세스내로 삽입이 되어 실행이 되며, 크게 2가지의 기능을 수행한다. 첫째, 복사 영역 검사로 프로세스 내부에서 영역을 복사하는 함수가 호출될 경우에 소스 영역이 보호해야할 뷰어의 영역들을 포함했는지 여부를 검사한다. 둘째, 이미지 캡쳐 무효화로 복사 영역 검사를 통해 소스 영역이 해당 사항이 있다면 복사 함수 호출을 무효화하여 이미지 복사가 이루어지지 않도록 한다.

4.2. 제안하는 DRM 시스템 흐름도



[그림 3] 제안 시스템의 흐름도

[그림 3]은 본 논문에서 제안하는 시스템의 흐름도를 나타낸 것이다. 캡쳐 방지 서버가 구동되면 가장 먼저 시스템 상에서 불법적인 이미지 복사 방지를 적용할 뷰어에 대한 정보를 얻는다. 다음으로 Windows 시스템 내에 기존 실행 상태로 존재하던 프로세스들을 체크하여 캡쳐 프로그램으로 의심 가능한 특정 라이브러리의 특정 함수를 포함한 프로세스들을 선별한다. 이때 새롭게 시작되는 프로세스들에 대해서도 동일한 기능을 수행하며, 선별된 프로세스들에 한해서는 캡쳐 방지 기능을 수행하는 캡쳐 방지 엔진을 삽입하게 된다. 프로세스에 삽입된 캡쳐 방지 엔진은 캡쳐 방지 서버로부터 자신이 보호해야할 뷰어의 정보를 얻어오며, 이미지 캡쳐를 위해서 필요한 특정 함수가 프로세스 내에서 호출이 된 경우에 해당 영역이 보호해야할 뷰어가 현재 존재하고 있는 영역과 겹쳐지는지를 검사한다. 검사를 통해서 뷰어의 영역과 겹쳐지는 부분이 있을 경우에는 영역 정보를 수정하거나 함수 호출 자체를 무효화함으로써 이미지 캡쳐가 이루어지지 않도록 한다. 마지막으로 불법적인 이미지 복사가 시도된 경우에는 해당 프로세스에 대한 정보를 캡쳐 방지 서버에게 전송한다. 캡쳐 방지 엔진으로부터 로그 정보를 받은 캡쳐 방지 서버는 이를 기반으로 로그 파일을 생성하게 된다.

5. 결론

본 논문에서 제안한 모델은 사용자의 PC환경에서 발생할 수 있는 캡쳐와 같은 불법적인 이미지 컨텐츠 접근 방법으로 효과적으로 컨텐츠를 보호할 수 있는 기능을 제공한다. 운영체제와의 연계를 통하여 컨텐츠를 보호하기에 기존의 소극적인 형태의 워터마킹이나 암호화를 통한 복제 방지에 비해서 효과적으로 이미지 컨텐츠 복제를 막을 수 있다. 현재 본 논문에서 제안 및 설계된 시스템은 구현 중에 있으며, 후에 오디오나 비디오와 같은 다른 종류의 컨텐츠에 대해서도 확장하여 적용하는 방법을 연구할 계획에 있다.

참조

[1] Raymond B. Wolfgang and Edward J. Delp, "A WATERMARK FOR DIGITAL IMAGES," IEEE International Conference on Image Processing (ICIP'96)

[2] Rachna Dhamija, and Fredrik Wallenberg, "A Framework for Evaluating Digital Rights Management Proposals," First International Mobile IPR Workshop: Rights Management of Information Products on the Mobile Internet, August, 2003

[3] S.Walton, "Information authentication for a slippery new age," Dr Dobbs Journal, vol. 20, no. 4, pp.18-26, April, 1995

[4] R. G. van Schyndel, A. Z. Tirkel, N. R. A. Mee, C. F.Osborne, "A digital watermark," Proceedings of the International Conference on Image Processing, November, 1994, Austin, Texas, vol. 2, pp. 86-90.

[5] J.-F. Delaigle, C. De Vleeschouwer, B. Macq, "Digital watermarking," accepted for publication, Journal of Electronic Imaging.

[6] DRM 포럼, http://www.drm.or.kr.