보안을 위한 무아레 무늬의 키 생성 기법

강혁[0], 최진영
고려대학교 컴퓨터학과
{paranblue, choi}@formal.korea.ac.kr

Key Generation Method using the Moire Patterns for Security

Hyeok Kang[0] JIN-Young Choi
Dept. of Computer Science & Engineering Korea University

요 약

현대는 인터넷의 범람이라고 할 수 있을 만큼 세계의 곳곳에서 많은 사람들이 인터넷을 통해 여러 분야에서 사용하고 있다. 이처럼 인터넷을 이용하는데 있어 개인의 정보를 보호해야 하는 문제가 대두되고 있다. 기존의 암호화에 사용하는 키는 소인수 분해, 이산수학, 타원곡선등과 같이 수학적 이론에 바탕을 두어 생성되었다. 본 논문에서는 빛의 물리적인 성질 중의 하나인 간섭과 회절에 의해 생성되는 고유의 무늬인 무아레 무늬의 고유 값을 암호화를 위한 키로 사용하도록 제안하였다.

1. 서 론

인터넷 사용자의 증가와 네트워크의 향상, 인프라의 보급 증가 등 다양한 전송 매체의 발달로 인하여 기존의 off-line을 통한 정보와 자료들의 이용이 인터넷을 통한 on-line이나 무선 환경을 통해서 쉽고 빠르게 이용할 수 있게 되었다. 요즘 무선 환경에서 사용할 수 있도록 각종 단말기 및 인터넷을 보급으로 무선 서비스를 이용하는 사용자가 지속적으로 증가하고 있다. 그러나 이러한 서비스를 지속적으로 활성화하기 위해서는 여러 가지 문제들이 산재되어 있는데 인터넷상에서 이용되어지는 정보나 자료, 사용자에 대한 보호 및 정보나 자료의 유료 서비스에 대한 결제 및 관리등과 같은 문제를 보다 안전하고 효과적으로 해결해야 한다. 특히 디지털 컨텐츠에 대한 불법 복사 및 배포, 그리고 변조등과 같은 불법적인 저작권 침해는 작게는 개인적인 재산권에 침해와 크게는 경제적으로 막대한 피해와 해당 서비스의 발전을 저해할 수 있다. 그러므로 디지털 컨텐츠를 제공하는 저작권자와 이 컨텐츠를 이용하는 사용자, 사용자의 권리를 보호할 수 있는 시스템을 개발해야만 한다. 디지털 정보의 지적 재산권 보호 방안으로, 먼저 기존 법체계에서의 저작권 보호를 생각해 볼 수 있다. 그러나 이러한 법적인 문제는 사후 구제수단의 역할을 할 뿐 실제적인 방지책이 될 수 없다는 한계를 갖는다. 따라서 이러한 법적인 보호만으로 무단 복제나 무단 이용으로 안전할 수 없기 때문에 실제적으로 재산권을 보호할 수 있는 기술적 방안이 요구된다. 이와 같이 지적 재산권 보호를 위한 기술로는 카피라이트 마킹과 스테가노그래피, 워터마킹등이 있으며 더 많은 기술적 방안들이 마련되어지고 있다. 이 논문에서는 디지털 컨텐츠를 전송할 때 보다 효과적이고 안전하게 인증 및 보호를 하기 위하여 빛의 고유의 성질인 간섭 및 회절에 의해 생성되는 무아레 무늬를 이용하였다. 이 무아레 무늬를 측정, 그 결과로 생성되는 데이터를 인증 시 필요한 랜덤 값으로 사용한다. 이 데이터 값은 빛의 파장의 단위로 생성되므로 광범위하고, 주위의 환경에 민감하게 반응하여 값이 다르게 됨으로 인증과정에 무엇보다도 고유성과 강인성을 필요로 되어지는 요건에 매우 적합하다. 따라서 본 논문은 기존의 디지털 저작권 보호에서 사용되어지는 소프트웨어에 의한 키 생성 방식과는 다른 하드웨어적으로 생성되는 키를 사용하여 보다 안전한 키 생성 및 이를 사용한 디지털 저작권 보호 시스템을 제안하였다.

2. 이론적 배경

2.1 Moire의 정의 및 현상

백색광 하에서 공간적으로 주기성을 갖는 반사판 또는 투과판을 서로 겹쳐 놓을 때 발생하는 물질 형태의 간섭무늬를 무아레 간섭무늬라고 하는데, 이러한 무아레 현상은 비간섭성 광원을 사용하는 강도(intensity)간섭 효과로 이해될 수 있다. 무아레 무늬는 주기적인 무늬가 겹쳐 나타나는 현상이다. 모기장 같은 망사 두 장이 겹쳐있을 때 망사를 이루는 세밀한 직물의 격자 간격보다 훨씬 크고 변화가 다양한 얼룩무늬를 볼 수 있다. 또한 머리 빗 두 개를 겹쳐서 보면 간격이 빗살보다 넓은 새로운 어두운 그림자를 볼 수 있다. 이렇게 주기적인 무늬를 무아레 무늬(Moire Fringe)라 한다. 이 Moire는 프랑스 말로 '물결 무늬'의 뜻을 가지고 있다[1,2].

무아레 간섭무늬의 형성은 이론적으로 공간상의 맥놀이 현상으로 설명될 수 있다 두 개의 유사한 공간상의 주기를 갖는 격자가 겹쳐진 상태를 공간상의 주파수 영역에서 살펴보면 원래의 격자들이 갖고 있던 고유의 주파수 성분들과 격자 주기의 합과 차에 해당되는 주파수 성분으로 분리할 수 있게 된다. 이때 격자 주파수의 차에 해당되는 저주파수 성분을 무아레 간섭무늬라 한다 [3,4].

[그림 1] 무아레 무늬의 예

2.2 디지털 저작권 관리(Digital Rights Management)

Digital Rights Management는 암호화 기술을 이용하여 허가되지 않은 사용자로부터 디지털 컨텐츠를 안전하게 보호함으로써 컨텐츠 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리하는 시스템으로 정의할 수 있다. 즉, 디지털 컨텐츠가 저작자 및 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 편리하게 유통될 수 있도록 제공되는 모든 기술과 서비스 절차 등을 포함하는 개념이다[5].

3. 제안한 시스템

3.1 무아레 무늬를 이용한 안전한 디지털 저작권 보호

본 논문에서 제안하는 무아레 무늬를 이용한 안전한 디지털 컨텐츠의 저작권 보호 시스템의 절차 및 흐름도는 다음과 같다.

① 시스템에서의 구성원들 간의 상호 인증을 위해서 DRM Server(CA)에서 무아레 무늬를 이용한 랜덤 값(random value) X를 생성한다. 이때 랜덤 값 X는 무아레 무늬에서 생성되어지는 3개의 차원(3-D)으로 구성되어진 값들(Radial position, Angular position, Intensity)을 집합으로 형성한 하나의 값이다.

② 시스템을 구성하고 있는 Publisher, Web server(provider), Finance, Users 모두 DRM sever에 등록 후 고유의 인증서를 받는다. 이때 받은 인증서에는 DRM Server에서 무아레 무늬에 의해서 생성된 랜덤 값 X를 포함한다. 본 논문에서 제안한 시스템은 이것을 전제로 한다.

③ 첫 번째로 Publisher는 컨텐츠를 생성하고, 자신이 생성한 키를 가지고 컨텐츠를 암호화한다. 이때 암호화된 컨텐츠에 DRM server로부터 받은 랜덤 값 X를 포함한다. 암호화된 컨텐츠를 Provider가 인터넷상에서 운영하는 Web server에 제공한다.

④. User A는 Provider가 운영하는 Web server로 회원 가입 후 Web에서 제공하는 컨텐츠 상품을 선택 후 다운로드 하는 컨텐츠에 대하여 여러 방식(신용카드, 인터넷 뱅킹, 핸드폰 결제 등)으로 결제를 한다.

⑤. 결제를 한 후 선택한 컨텐츠를 다운로드 한다.

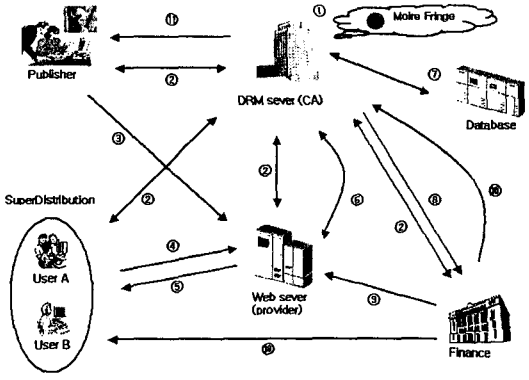
⑥. User가 Web server에서 컨텐츠를 사용한 정보와 결제 정보를 Web server가 DRM server에게 제공한다.

⑦. DRM server는 Web server에게 받은 정보에 무아레 무늬에 의해 생성된 랜덤 값 X를 있는 지 확인 후 DRM server가 운영하는 Database에서 랜덤 값 X의 매칭(matching)하여 사용자의 신원을 확인한다.

⑧. 정당한 사용자라고 인증되면 DRM server는 Finance에 컨텐츠 값에 대한 결제를 요청한다.

⑨. Finance는 결제 요청을 하는 DRM server가 정당한지 인증을 한 후 이 인증과정이 정당하다고 하면 대금을 Web server에게 실질적인 금액을 결제하여 준다.

⑩. 마지막으로 DRM server는 Publisher에게 Finance에게 받은 결제 대금 정보 및 사용내역을 제공한다.



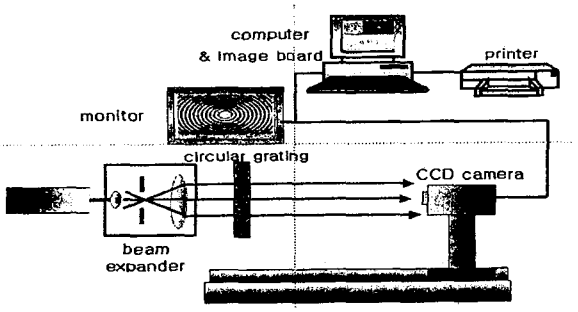
[그림 2] 제안한 시스템의 흐름도

본 논문에서는 일반적인 DRM 시스템에서 들어가 있는 Clearinghouse의 역할을 DRM server에 부여함으로써 처리 과정을 보다 간단하게 하였다. Clearinghouse가 수행해야 하는 User와 Finance, Web server와는 별도의 인증과정이 필요하고 이에 대한 각각 개별적인 키를 사용해야 하는 것을 DRM server에서 생성한 랜덤 값 X 하나로 모든 구성 요소들의 인증을 확인할 수 있다는 장점을 가진

다.

그러나 단 하나의 랜덤 값으로 모든 절차들을 인증하기 때문에 절대적으로 강인성을 지닌 랜덤 값이 필요하다.

3.2 무아레 무늬를 생성 장치



[그림 3] 무아레 무늬 생성 장치

[그림 3]는 무아레 무늬를 생성하기 위한 실험 장치도이다. 보통의 무아레 무늬는 비간섭성 광원, 즉 보통의 태양 빛이나 현광등, 백열전등의 빛으로도 무아레 무늬는 생성된다. 그러나 더 정확한 무늬를 생성하기 위하여 이 실험에서는 레이저를 사용하였다. 레이저의 빛은 beam expander 안의 작은 구멍은 통하여 확산된다. 이 확산된 빛은 미리 준비해둔 원형 격자(circular grating)를 통과하면서 간섭을 일어나면서 무아레 무늬가 생성된다. 이때 생성되는 무늬를 CCD 카메라가 촬영하고 이 영상 모니터 하여 컴퓨터에서 분석을 한다. 무아레 무늬를 나타내는 데이터는 3개의 축으로 구성되어진 값들로 이우러져 있다. 즉 Radial position과 Angular position, 마지막으로 빛의 Intensity이다. 본 논문에서는 두 개의 원형격자를 이용하여 생성되는 랜덤 값을 이용하였다. 두 개의 원형 격자가 서로 이동하면서 생기는 무아레 무늬를 표현하기 위해서는 3개의 값들이 일치를 하여야 한다. 이것은 빛의 성질을 이용하여 생성되어진 값이기 때문에 일치한 값을 찾기란 무척 어렵다. 본 논문에서는 이러한 무아레 무늬가 일치하는 값을 갖기 어렵다는 성질을 이용하였다.

4. 결론 및 향후 연구과제

급속도로 성장해가는 디지털 컨텐츠 산업에 있어서 주요 자료와 개인 정보들에 대한 도청, 위·변조 및 신분 위장 등 불법적인 범죄가 더욱 증가할 것이다. 이를 방지하기 위해서는 보다 안전하고 효율적인 인증 방법을 개발하는 것이 중요하다고 생각한다. 실제로 암호화된 디지털 컨텐츠를 해킹하는 방법은 다양하게 존재하고 있다.

기존의 DRM 시스템에서 키를 소프트웨어적인 방법으로 생성하는 반면 본 논문에서는 하드웨어적인 방법으로 키를 생성하는 방법을 채택하였다. 즉 빛의 고유의 성질인 간섭 및 회절 현상에 의해 생성되는 무아레 무늬의 3차원 데이터를 하드웨어적인 실험에 의하여 생성하여 다른 디지털 컨텐츠 보호에 쓰이는 암호 키보다 키의 복잡성과 조금의 환경 조건에 의해서도 변화에 크게 민감하여 강인성을 지닌다는 성질을 이용하여 컨텐츠 저작자와 사용자, 유통업자 사이의 인증에 사용되는 키로 이용함으로써 기존의 디지털 컨텐츠 보호 시스템에서 사용하는 키 생성 방식과는 전혀 다른 새로운 키 생성에 의한 안전한 시스템으로 제안하였다.

향후 본 논문에서 언급하지 않았던 시스템 프로토콜을 구현하여 현실에 적용할 수 있는 연구가 되어야 할 것이며, 무아레 무늬에서 생성되는 데이터를 가지고 상호 인증에만 사용하는 것이 아니라 원래의 영상에 무아레 무늬를 직접 삽입하여 직접적으로 보이는 영상에도 영향을 줄 수 있어 보다 견고하고 안전한 컨텐츠 보호의 연구가 되어야 할 것이다.

5. 참고 문헌

[1] Fabien A.P Petitcolas, Ross J. Anderson and Markus G.Kuhn, "Information Hidden - A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, May 1999. Invited paper.

[2] Neil F. Johnson, Sushil Jajodia. "Exploring Steganography : Seeing the Unseen".

[3] Schneier, B., Applied Cryptography, New York, USA :John wiley & Sons, 2nd ed., 1996.

[4] 김일환, 육근철, 조재홍, 장수 "두 원형 격자의 무아레 간섭무늬를 이용한 회전각 측정" 새물리 32,674-678, 1992.1989)

[5] Joshua, D., "Digital Rights Management" , IDC, 2001