RFID기반 디지털 컨텐츠 인증 기법

양정규*, 배성우*, 정명섭*, 이재문**, 김준형***, 이윤덕****, 장윤석*****, 오하령*, 성영락*, 박준석*
국민대학교 전자공학과*
한성대학교 멀티미디어 공학과**
경희 대학교 교육대학원***
연세대학교 전자공학과****
항공대학교 항공교통물류학부*****

Digital contents authentication scheme based on RFID technology

Jung-Kyu Yang*, Sung-Woo Bae*, Myung-Sub Jeong*, Jae-Moon Lee**, Jun-Hyung Kim***,
Yoon-Deock Lee****, Yoon-Seok Chang*****, Ha-Ryoung Oh*, Yeong-Rak Seong*, Jun-Seok Park*
Dept. of Electronic Engineering, Kookmin University*
Dept. of Multimedia Engineering, Hansung University**
The graduate school of education, Kyunghee University***
School of Electronic Engineering, Yonsei University****
School of Air Transport, Transportation and Logistics, Aerospace University*****

Abstract - 디지털 사회에서는 정보 기술의 발전에 따른 다양한 디지털 컨텐츠들이 필요하고 수많은 디지털 컨텐츠들이 다양한 용도로 사용되고 있다. 그러나 불법복제로 인해 저작권자의 지적재산권을 침해받는 문제가 부각되면서 디지털 컨텐츠의 저작권을 보호하기 위한 많은 기술들이 개발되고 있다. 그 중 DRM은 가장 최적의 기술로 평가되고 있으며 이미 다양한 분야에서 사용되고 있다. DRM을 구성하는 기술 중에 인증기술은 불법복제를 방지하고 저작권을 보호하기 위한 핵심기술이다. 본 논문에서는 DRM의 기존 인증기술들이 가지고 있는 문제점을 해결하기 위하여 RFID기술을 이용하였다. 제안한 인증 기법은 RFID 태그에 저장된 디지털 컨텐츠의 인증 정보와 디지털 컨텐츠에 저장되어진 인증 정보를 주기적으로 비교하여 인증 여부를 결정한다. RFID 태그는 쉽게 복제될 수 없기 때문에 디지털 컨텐츠의 저작권을 효과적으로 보호할 수 있다.

1. 서 론

최근 음악, 비디오, 소프트웨어 등과 같은 수 많은 디지털 컨텐츠들이 인터넷을 통해 유통되고 있다. 디지털 컨텐츠는 무한히 반복하여 사용해도 품질이 저하되지 않고 수정과 복사가 편리 하다. 그러나 네트워크를 통해 불법 복제된 컨텐츠를 짧은 시간에 배포할 수 있기 때문에 지적재산권자의 권리를 위협하는 원인이 되기도 한다. 이 문제는 디지털 컨텐츠 산업의 성장을 가로막는 가장 큰 장애물이다.

이러한 문제를 해결하기 위해서 많은 기술들이 발표되었다. 그 중 DRM기술이 최적의 기술로 평가되고 있다[1-4]. DRM은 인증(Authentication), DRM 패키징 포맷(Secure Container), 디지털 컨텐츠 식별체계(Identification), 메타데이타(Meta-Data), 디지털 워터마킹(Digital Watermarking) 등의 기술들이 조합되어 구성되며, 그 중 인증기술은 불법복제를 방지하고 저작권을 보호하기 위한 핵심기술이다. 현재 DRM의 인증기술로는 ID/Password, CPU 고유번호, MAC address, Hard-lock Key, Symmetric/Asymmetric Cryptographic등을 이용한 방법들이 있다.

본 논문에서는 DRM의 기존 인증기술들이 가지고 있는 문제점을 해결하기 위하여 RFID기술을 이용하였다. 제안한 인증 기법은 RFID 태그에 저장된 디지털 컨텐츠의 인증 정보와 디지털 컨텐츠에 저장되어진 인증 정보를 주기적으로 비교하여 인증 여부를 결정한다. 만약 이 두 정보가 같거나 상관관계가 존재하면 디지털 컨텐츠를 사용할 수 있으며 그렇지 않은 경우에는 디지털 컨텐츠의 사용이 불가능하다.

RFID 시스템은 리더와 태그로 구성되며 무선 통신을 통해 리더와 태그간의 정보를 송수신할 수 있는 기술이다. RFID 기술은 많은 장점을 가지고 있지만, 비 접촉식이라는 RFID 특성상 도청 등으로 인해 중요한 정보가 노출될 수 있는 문제점도 가지고 있다. 이를 해결하기 위해 많은 기법들이 제안되었지만 도청 공격(eavesdropping attack), 재전송 공격(replaying attack), 스푸핑(spoofing attack) 등에 취약하여 보안 문제를 완전하게 해결하지 못하고 있다[5]. 그러나 제안한 인증 기법은 비가역적 함수(one-way function)가 구현된 특수한 RFID 태그와 랜덤넘버를 이용하여 문제를 해결하였다.

디지털 컨텐츠는 복제할 수 있지만 RFID 태그는 복제할 수 없기 때문에 불법 복제된 디지털 컨텐츠는 인증을 받을 수가 없으므로 사용이 불가능하다. 이를 통해 제안한 인증 기법은 디지털 컨텐츠의 저작권을 효과적으로 보호할 수 있다.

2. 관련 연구

2.1 Digital Rights Management

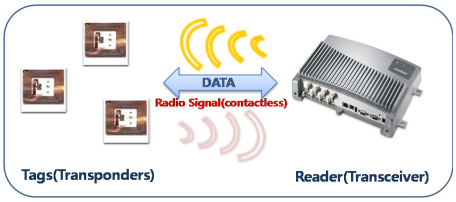
DRM(Digital Rights Management)은 전자책, 음악, 비디오, 소프트웨어등의 각종 디지털 컨텐츠를 불법복제로부터 보호하고 요금을 부가하여 저작권 관련 당사자에게 발생하는 이익을 관리하는 상품과 서비스를 말한다. DRM은 단순 보안기술보다는 좀 더 포괄적인 개념으로 저작권 승인과 집행을 위한 소프트웨어와 보안기술, 지불, 결제기능 등이 모두 포함된다. 즉 보안의 경우는 한번 암호를 풀면 누구든 해독된 파일이나 컨텐츠를 이용할 수 있지만 DRM은 각각의 사용자 모두가 사전에 정해진 조건을 만족해야만 이용할 수 있는 장치로 특정 파일을 인터넷에서 내려받아 요금을 지불하고 감상한 후 다른 사람에게 전송해 주었더라도 전송받은 사람도 파일을 열어보기 위해서는 별도의 요금을 지불해야 하는 시스템이다. 즉 컨텐츠의 자유로운 복제는 허용하되 불법 사용은 철저히 막는 것이 DRM의 목적이다.

DRM은 인증(Authentication), DRM 패키징 포맷(Secure Container), 디지털 컨텐츠 식별체계(Identification), 메타데이타(Meta-Data)등의 기술들이 조합되어 구성된다. 인증 기술은 허가된 사용자 또는 장치에서만 사용 권한이 유효하도록 통제하기 위해 사용되는 기술이다. 디지털 컨텐츠 식별체계, 메타데이터 기술을 이용하여 유통과정에서의 컨텐츠 관리를 용이하게 하고 디지터 컨텐츠의 보호 및 신뢰성 있는 유통을 위해 DRM 패키징 포맷 기술을 이용한다[1-4].

2.2 RFID 기술 개요

일반적으로 RFID 시스템은 <그림 1>과 같이 태그, 리더로 구성된다.

RFID(Radio Frequency Identification) 기술은 무선 주파수를 이용하여 물리적인 접촉 없이 개체에 대한 정보를 읽거나 쓰는 자동인식 기술 시스템이다. 바코드에 비해서 저장 능력이 뛰어나고 비 접촉식이라는 점에서 바코드를 대체할 자동 인식 시스템으로 주목 받으면서 많은 연구가 이루어지고 있다.



<그림 1> RFID 시스템의 구성

2.3 RFID기반 디지털 컨텐츠 인증 시스템의 요구 사항

RFID 기술을 디지털 컨텐츠 인증 시스템에 적용하기 위해서는 일반적인 디지털 컨텐츠 인증 시스템들이 가져야하는 요구사항 외에 RFID 기술이 가지는 취약점에 대비한 요구사항도 만족해야 한다.

일반적으로 디지털 컨텐츠 인증시스템은 다음의 사항을 만족해야 한다. 첫 번째는 디지털 컨텐츠를 유료화하는데 있어 중요한 용도로서 불법 복제를 방지해 디지털 컨텐츠가 가진 상업적인 가치를 보호하는 것이다. 두 번째는 보안에 가까운 개념으로 컨텐츠가 가진 기밀성을 보호해야 한다. 세 번째는 판매목적이 아닌 학술 논문이나, 사진등과 같은 컨텐츠의 지적재산권을 보호해야 한다. 마지막으로 유통과정에서디지털 컨텐츠가 변형, 훼손, 수정되지 않고 무결성을 보장해야 한다.

또한 RFID 기술의 보안적인 취약점을 제거하기 위해 다음의 기능을 가져야 한다[5-6].

1) 도청공격(Eavesdrop) 대처능력 : 공격자가 리더와 태그사이의 통신을 도청하더라도 태그에 저장된 중요한 정보를 알아내는 것이 불가능해야 한다.

2) 재전송공격(Replay Attack) 대처능력 : 공격자가 태그와 리더간의 통신 중에 수집한 내용을 가지고 리더로부터 인증을 받아서는 안 된다.

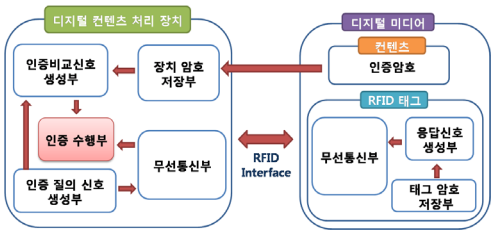
3) 스푸핑공격(Spoofing Attack) 대처능력 : 공격자가 리더나 태그로 위장하여 비밀정보를 알아내는 것이 불가능해야 한다.

2.4 기존 RFID 인증 기법의 문제점 분석

RFID 시스템에서 정보 보호를 위해 다양한 기법들이 제안되었다[5-6]. 이 중 해쉬함수 기반 기법을 이용한 많은 연구가 이루어지고 있지만 아직 문제점이 있다. 예를 들어 해쉬 락 기법[5]은 태그가 소유한 ID를 숨기기 위해 metaID를 이용하지만, metaID가 고정 값이기 때문에 공격자에 의한 스푸핑이 가능하다는 단점이 있다. 이를 보안하기 위해 Randomized 해쉬 락 기법[5]이 제안 되었으나 종료 과정에서 실제 ID가 노출된다는 문제점이 있다. 이에 다시 해쉬 체인 기법[6]이 제안되었으나, 서로 다른 두개의 해쉬함수를 사용해서 매번 리더의 요청에 대한 태그의 응답하는 값이 다르기 때문에 전송되는 값이 노출되어도 공격에 대해서 안전하다. 그러나 Back-end 서버에서의 계산이 늘어나는 단점이 있다. 또한 비트연산 기반 기법과 재 암호화 기법들은 Back-end DB, 재암호화 장치에 대한 별도의 인프라가 필요하다는 단점이 있다.

3. RFID기반 디지털 컨텐츠 인증

3.1 시스템 구성



<그림 2> 시스템 블록도

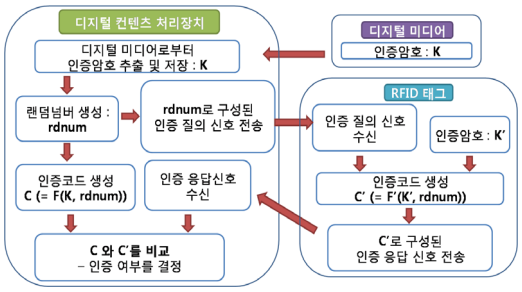
<그림 2>와 같이 디지털 컨텐츠 인증처리 시스템은 디지털 컨텐츠 처리장치와 RFID태그가 부착된 미디어(Media)로 구성된다.

디지털 컨텐츠 처리장치는 디지털 미디어에 저장된 데이터를 읽을 뿐만 아니라 디지털 미디어에 부착된 태그와 통신을 한다. 이 장치는 인증 질의 신호 생성부, 장치 무선 통신부, 인증 수행부, 인증 비교 신호 생성부, 장치 암호 저장부로 구성된다. 장치 암호 저장부는 디지털 미디어로부터 인증 암호(K)를 추출하여 저장한다. 인증 질의 신호 생성부는 랜덤넘버(rdnum)를 이용하여 인증용 질의 신호를 생성한다. 인증 비교 신호 생성부는 인증 암호(K), 랜덤넘버(rdnum), 비가역적 함수(one-way) F를 이용하여 인증코드(C)를 생성한다. 무선통신부는 인증 질의 신호를 송신하고 인증 응답 신호를 수신하다. 인증 수행부는 인증코드(C)와 태그로부터 수신한 인증 코드(C′)을 비교하여 인증여부를 판단한다.

제안한 인증 기법의 RFID 태그는 일반적인 RFID 태그와는 달리 비가역적 함수가 구현된 특수한 태그이다. 이 태그는 인증 응답 신호 생성부, 무선 통신부, 태그 암호 저장부로 구성된다. 태그 암호 저장부는 인증암호(K′)를 저장하고 있고 인증 응답 신호 생성부는 태그의 인증 암호(K′), 디지털 컨텐츠 처리 장치로부터 수신한 랜덤넘버(rdnum), 비가역적 함수(one-way) F′를 이용하여 인증코드(C‘)를 생성한다. 무선통신부는 인증 질의 신호를 수신하고 인증 응답 신호를 송신한다. 그리고 인증암호(K′)가 저장되어 있는 영역은 쉽게 접근할 수 없는 영역이다.

디지털 컨텐츠 처리 장치의 인증 비교 신호 생성부와 장치 암호 저장부는 태그의 응답 신호 생성부와 태그 암호 저장부와 각각 대응된다. 그러나 태그 암호 저장부의 인증암호는 바꾸지 않는 반면 장치 암호 저장부의 인증 암호는 디지털 미디어가 로드(load)될 때 마다 매번 바뀐다. 그리고 인증 응답 신호 생성부는 하드와이어드(hard-wired) 디지털 로직 회로로 비가역적 함수(one-way)가 구현되어 있지만 인증 비교 신호 생성부는 소프트웨어로 구현되어 있다.

3.2 인증 처리 방법



<그림 3> 인증처리절차

<그림 3>은 디지털 컨텐츠 인증 처리 절차를 보여주고 있다. 여기서 인증 암호는 두 군데 영역에 각각 저장된다. 첫 번째 인증암호는 디지털 미디어 내에 미리 정의된 특정 위치에 저장되어 있고 두 번째 인증 암호는 디지털 미디어에 부착된 RFID 태그의 쉽게 접근할 수 없는 특수 영역에 저장되어 있다. 두 개의 인증 암호는 서로 같을 수도 있고 다를 수도 있다.

디지털 컨텐츠 처리 장치에 디지털 미디어가 로드되면 장치 암호 저장부는 디지털 미디어로부터 인증 암호(K)를 추출하고 저장한다. 그리고 인증 질의 신호부에서 인증 질의 신호(rdnum)을 생성하고 무선 통신부는 태그로 인증 질의 신호를 송신한다. 디지털 처리 장치는 증 암호(K), 랜덤넘버(rdnum), 비가역적 함수(one-way) F를 이용하여 인증코드(C=F(K, rdnum))를 생성한다. 태그는 수신한 인증 질의 신호(rdnum)와 태그 암호 저장부에 저장된 인증 암호(K′), 비가역적 함수(one-way) F′를 이용하여 인증 코드(C′=F′(K′, rdnum))를 생성한다. 태그 무선 통신부는 인증 응답 신호를 디지털 컨텐츠 처리 장치로 송신한다. 인증 수행부에서는 인증코드(C)와 수신한 인증 코드(C′)을 비교하여 인증 여부를 결정한다. 만약 이 두 정보가 같거나 상관관계가 존재하면 디지털 컨텐츠를 사용할 수 있으며 그렇지 않은 경우에는 디지털 컨텐츠의 사용이 불가능하다.

3.3 시스템 분석

디지털 미디어의 특수 영역에 저장되어 있는 인증 암호(K)를 공격자(attacker)가 알아내어 디지털 미디어를 불법 복제할 수 있더라도 RFID 태그는 복제할 수 없다. 그러므로 불법 복제된 디지털 미디어는 디지털 컨텐츠 장치로부터 인증을 받을 수 없으므로 사용할 수 없다.

또한 공격자가 디지털 컨텐츠 처리 장치의 무선 통신부와 RFID 태그의 무선 통신부 사이의 통신 내용을 도청하여 분석할 수도 있다. 통신 도중에 노출되는 정보는 인증 질의 신호와 인증 응답 신호이다. 인증 질의 신호는 랜덤 넘버(rdnum)을 이용하여 생성되기 때문에 인증 응답 신호는 매번 변한다. 만약 공격자가 인증 질의 신호에 따른 모든 인증 응답 신호를 알수 있다면 불법 복제가 가능할 수 있다. 그러나 랜덤 넘버(rdnum)가 64비트일 경우에는 인증 응답 신호의 경우의 수는 2^{64} (대략 18×10^{18})이다. 2^{64}는 1800경의 크기를 가지는 수이기 때문에 현실적으로 모든 응답 신호의 경우의 수를 분석하는 것은 불가능하다. 만약 모든 경우의 인증 응답 신호를 알고 있더라도 이를 상업적인 태그에 구현하는 것은 불가능하다.

이를 통해 제안한 디지털 컨텐츠 인증 기법은 디지털 컨텐츠의 저작권을 효과적으로 보호할 수 있다.

4. 결 론

디지털 컨텐츠 사회에서 저작권을 보호하는 것은 매우 중요하다. 본 논문에서는 RFID 기술을 이용한 디지털 컨텐츠 인증 기법을 제안하였다. 이 인증 기법은 비가역적 함수(one-way function)를 하드와이어드(hard-wired) 디지털 로직 회로를 구현한 특수한 태그를 이용하였다. 이 RFID 태그는 쉽게 복제할 수 없기 때문에 디지털 컨텐츠의 저작권을 효과적으로 보호할 수 있다.

제안한 인증 기법을 기존 DRM 기술들과 잘 조합하여 이용한다면 디지털 컨텐츠 불법 복제 방지 및 저작권자의 지적재산권 보호하는데 도움이 될 것으로 기대된다.

감사의 글

본 연구는 구원장학재단 연구비지원에 의해 수행되었습니다.

[참 고 문 헌]

[1] Eberhard Becker, Willms Buhse, Dirk G□unnewig, Niels Rump, "DRM as an Inerlocking Challenge for different Scientific Disciplines - Introduction", pages 1-3. Number 2770 in LNCS. Springer-Verlag Heidelberg, November 2003.

[2] Niels Rump, "Digital Rights Management - Definition, Aspects and Overview", pages 3-16. Number 2770 in LNCS. Springer-Verlag Heidelberg, November 2003.

[3] Gabriele Spenger, "Digital Rights Management -Authentication, Identification Techniques and Secure Containers", pages 62-82. Number 2770 in LNCS.

[4] Susanne Guth, "Digital Rights Management - Rights Expression Languages", pages 101-113. Number 2770 in LNCS.
Springer-Verlag Heidelberg, November 2003.

[5] S. Weis, Sarma, R. Rivest and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", in 1st Intern. Conference on Security in Pervasive Computing(SPC), 2003

[6] M. Ohkubo, K. Suzuki and S. Kinoshita. "Efficient Hash-Chain Based RFID Privacy Protection Scheme", Ubcomp2004 workshop.